Capabilities of Bounded Discrepancy Decoding

By A. D. WYNER

(Manuscript received February 23, 1965)

The following four channels are considered: (A) a class of discrete memoryless channels with q inputs and outputs, (B) the time-discrete, amplitude-continuous memoryless channel with additive Gaussian noise and amplitude constraint, (C) the same as channel B but with energy instead of amplitude constraint, (D) a class of time-discrete, amplitude-continuous memoryless channels with amplitude constraint and non-Gaussian noise. For each channel the theoretical capabilities of "bounded discrepancy decoding" are studied.

The "discrepancy" between two vectors is a distance or distance-like quantity defined such that the optimal decoder is a "minimum discrepancy decoder." For example, for channel A the discrepancy is the Hamming distance, and for channel B the discrepancy is the Euclidean distance. Bounded discrepancy decoding is a nonoptimal decoding scheme in which disjoint regions in the space of possible received vectors are constructed about each code word, each region consisting of those vectors within a fixed discrepancy of that code word. For example, in channels A and B the regions are spheres with centers at the code words and radius $d/2$ where d is the minimum distance between code words. If the received vector is in the region about code word i, it is decoded as code word i; otherwise the decoder announces an error.

For all four classes of channels the following is shown to hold: There exists a fixed positive rate C_B below which it is possible (asymptotically in n) to obtain exponentially small error probability using bounded discrepancy decoding. In many cases C_B is shown to be strictly less than the channel capacity.

TABLE OF CONTENTS

I. INTRODUCTION

To fix ideas, let us consider first the special case of coding for the binary symmetric channel. A *code* is defined as a set of M binary n-vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ where $x_k = 0$ or 1 $(k = 1, 2, \ldots, n)$. The individual vectors are called code words. The transmission rate R is defined by $M = 2^{nR}$. The *Hamming distance* between two binary n-vectors is the number of positions in which they differ.

The code words are transmitted through a noisy channel. The received vector $\mathbf{y}$ is a binary n-vector whose kth coordinate is

$$y_k = x_k + z_k \pmod 2, \qquad k = 1, 2, \ldots, n, \tag{1}$$

where x_k is the kth coordinate of the transmitted code vector, and the z_k $(k = 1, 2, \ldots, n)$ are statistically independent random variables which assume the value 1 with probability $p_o (0 \leqq p_o \leqq \frac{1}{2})$, and the value 0 with probability $1 - p_o$. Thus p_o is the probability that a given bit is received in error. This channel is the "binary symmetric channel." It is assumed that each of the M code words is equally likely to be transmitted, and it is the task of the decoder to examine the received vector $\mathbf{y}$ and decide which code word was actually transmitted. We are interested in two types of decoding.

The first is termed *minimum distance decoding* or *minimum discrepancy decoding* (MDD), and here the decoder selects that code word which has the smallest Hamming distance from the received vector, and announces that word as the one which was transmitted. It is not hard to show that MDD is optimum in the sense that it minimizes the average probability of error for a given code. Let us denote by P_{eM} the average probability of error using MDD. The Fundamental Theorem of Information Theory[1] states that for any rate R less than the channel capacity $C = 1 + p_0 \log_2 p_0 + (1 - p_0) \log_2 (1 - p_0)$, there exists a sequence of n-dimensional codes (one for each n) with rate R such that $P_{eM} \to 0$, as $n \to \infty$. Further we may write $P_{eM} = 2^{-nE(R)+o(n)}$ where $E(R) > 0$ when $R < C$. Estimates of the exponent $E(R)$ have been found.[2,3,4]

In order to construct specific codes many workers (for example, see Refs. 5 and 6) have considered codes in which the minimum Hamming distance between code words is d. Such codes are capable of correcting errors affecting $e = (d - 1)/2$ or fewer coordinates. Suppose that the code under consideration has minimum distance d and that the decoder corrects *only* errors corrupting $e = (d - 1)/2$ or fewer coordinates (and announces an error if the received vector is not within Hamming distance e of some code word). We term this type of decoding *bounded distance decoding* or *bounded discrepancy decoding* (BDD) and the resulting error probability P_{eB}.† Since BDD does not exploit the full error-correcting potential of the code (an error may corrupt more than $e = (d - 1)/2$ coordinates and still be correctable using MDD) it is clear that $P_{eB} \geqq P_{eM}$. In this paper we shall study the theoretical capabilities of BDD, and show quantitatively what is lost by using BDD instead of MDD.

For the binary symmetric channel the following will be shown to hold:

Theorem A: There exists a fixed rate C_B (called the bounded distance decoding channel capacity*) below which it is possible (asymptotically in n) to obtain exponentially small error probability using BDD. In other words, for every $R < C_B$, there exists a sequence of n-dimensional codes (one for each n) with rate R such that $P_{eB} = 2^{-nE_B(R)+o(n)}$ where $E_B(R) > 0$ if $R < C_B$). Further if $R > C_B$, $P_{eB} \to 1$ as $n \to \infty$.*

Although C_B is not known exactly, it can be shown to satisfy

† The Peterson-Chien algorithm for decoding Bose-Chaudhuri-Hocquenghem codes is an example of BDD. (See Chien, R. T., Cyclic Decoding Procedures for Bose-Chaudhuri-Hocquenghem Codes, IEEE Trans. on Information Theory, *IT-10*, 1964, pp. 357–363).

$$1 - H(2p_o) \leqq C_B \leqq 1 - H(\tfrac{1}{2} - \tfrac{1}{2}\sqrt{1 - 4p_o}), \qquad (2)$$

where $H(\rho) = -\rho \log_2 \rho - (1 - \rho) \log_2 (1 - \rho)$, and p_o is the bit error probability of the binary symmetric channel. These upper and lower bounds on C_B are plotted vs p_o in Fig. 1. It is clear that C_B is bounded below the channel capacity C, the maximum "error-free rate" obtainable using (optimum) MDD. The exponent $E_B(R)$ can also be estimated by upper and lower bounds.

In this paper we shall study a number of different channels (continuous as well as discrete). For each channel we shall define a distance-like function called the "discrepancy" which will be chosen so that the optimum decoder is a "minimum discrepancy decoder." (For the binary symmetric channel the discrepancy is the Hamming distance, and in most of the cases to be considered the discrepancy is a metric.) We then define a "bounded discrepancy decoder" and compare the capabilities of BDD to those of optimal MDD. In all cases we will deduce the existence of a "bounded distance decoding channel capacity" C_B for which Theorem A holds. In many of these cases we will show that C_B is strictly less than the channel capacity.

A glossary of symbols is included at the end of the paper.

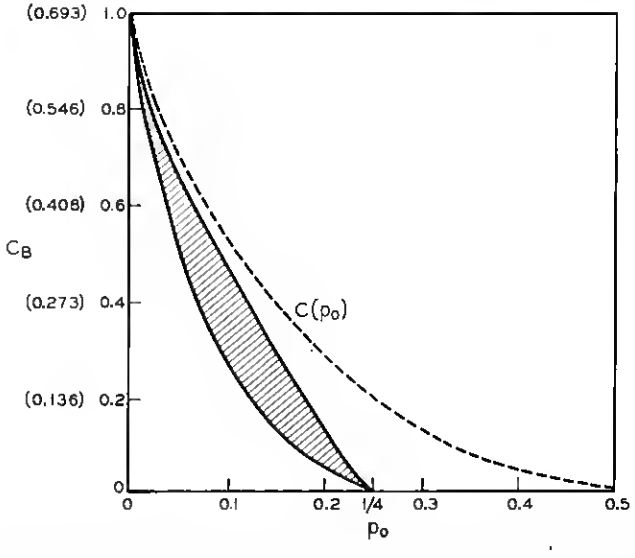

Fig. 1 — Upper and lower bounds on C_B (2) (in bits) for binary symmetric channel (solid lines). Thus C_B lies in the shaded area. The channel capacity C is the dotted line. The equivalent value of C_B corresponding to natural logarithms is given in parenthesis.

II. SUMMARY OF RESULTS

We shall consider four classes of channels. In each case the input and output are n-vectors $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ and $\mathbf{y} = (y_1, y_2, \cdots, y_n)$ respectively, related by

$$y_k = x_k + z_k, \qquad k = 1, 2, \cdots n. \tag{3}$$

The symbols x_k, y_k and the noise digits z_k are as follows:

Channel A (Diserete Channel): The input digits x_k $(k = 1, 2, \cdots, n)$, the output digits y_k $(k = 1, 2, \cdots, n)$, and tbe noise digits z_k $(k = 1, 2, \cdots, n)$ are members of the finite alphabet of q symbols, $0, 1, \cdots, q-1$. The addition in (3) is modulo q. The z_k are independent random variables assuming the value 0 with probability $1 - p_o$, and the values $1, 2, \cdots, q-1$ with probability $p_o/(q-1)$. Thus the channel transmits each symbol correctly with probability $1 - p_o$, and makes an error with probability p_o, all errors being equally likely. The *Hamming distance* $d_H(\mathbf{u},\mathbf{v})$ between two n-vectors $\mathbf{u}$ and $\mathbf{v}$ with entries from the alphabet of q symbols is the number of positions in which $\mathbf{u}$ and $\mathbf{v}$ differ.

Channel B (Gaussian Channel with Amplitude Constraint): The digits x_k, y_k, z_k $(k = 1, 2, \cdots, n)$ are real numbers. The input vector $\mathbf{x}$ satisfies an amplitude constraint:

$$-A \leqq x_k \leqq +A, \qquad k = 1, 2, \cdots, n. \tag{4}$$

The noise digits z_k $(k = 1, 2, \cdots, n)$ are independent Gaussian random variables with mean zero and variance N. The Euclidean distance between two vectors $\mathbf{u}$ and $\mathbf{v}$ is denoted by $d_E(\mathbf{u},\mathbf{v})$.

Channel C (Gaussian Channel with Energy Constraint): The digits x_k, y_k, z_k $(k = 1, 2, \cdots, n)$ are real numbers. The input vector $\mathbf{x}$ lies on the surface of the n-dimensional hypersphere with center at the origin and radius $\sqrt{nP}$. Thus

$$\sum_{k=1}^{n} x_k^2 = nP. \tag{5}$$

As in ehannel B, the noise digits z_k $(k = 1, 2, \cdots, n)$ are independent Gaussian random variables with mean zero and varianee N. The signal "energy" is $\sum x_k^2 = nP$, and tbe expected noise "energy" is

$$E\left(\sum_k z_k^2\right) = nN,$$

so that the signal-to-noise energy ratio is P/N. This quantity is also the ratio of signal-to-noise "average power."

Channel C is of course closely related to the bandlimited channel with white Gaussian noise.[1] Such an identification, however, must be made with care, and we shall sidestep the issue here.

Channel D (Continuous Channel with Amplitude Constraint): The vectors $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ are members of $\mathcal{C}_n$ defined as the set of n-vectors $\mathbf{u} = (u_1, u_2, \cdots, u_n)$ where the coordinates u_k $(k = 1, 2, \cdots, n)$ are real numbers satisfying

$$-A \leqq u_k \leqq A. \tag{6}$$

We shall assume that the symbols "$\dotplus$" and "$\dot{-}$" when applied to coordinates of vectors in $\mathcal{C}_n$ denote addition and substraction modulo $2A$, with the result reduced into the interval $[-A,A]$. Equation (3) will thus be rewritten as

$$y_k = x_k \dotplus z_k, \qquad k = 1, 2, \cdots, n. \tag{7}$$

The noise coordinates z_k are assumed to be independent identically distributed random variables with probability density function $p(u)$ which satisfies:

(8)
- (a) $p(u) = 0, \quad |u| > A.$
- (b) $p(u) > 0, \quad |u| \leqq A.$
- (c) $p(u)$ is an even function of u.
- (d) $p(u)$ is a continuous, strictly monotone decreasing function of u for $0 \leqq u \leqq A$.
- (e) There exists an $\alpha > 0$ such that for small u we may write

$$p(u) = p(0)[1 + O(u^{\alpha})].$$

Thus what we have done is to wrap the interval $[-A,+A]$ onto the circumference of a circle, and assume that the noise perturbs each coordinate along the circumference a distance z_k $(-A \leqq z_k \leqq A)$. Such a channel is reasonable for the case where the x_k correspond to the phase of a fixed waveform,† and also as an approximation to other channels.

For each channel we define a *code* as a set of M n-vectors $\mathbf{x}$ satisfying the above constraints. The transmission rate R is defined by $R = (1/n) \ln M$‡ so that $M = e^{nR}$ We assume that each of the M code words is equally likely to be transmitted. It is the task of the decoder to examine the received vector $\mathbf{y}$ and to decide which code word was actually

† An example in which this model is applicable may be found in A. J. Viterbi, "On a Class of Polyphase Codes for the Coherent Gaussian Channel," *IEEE International Convention Record*, part 7, 1965, pp. 209–213.

‡ For the remainder of this paper all logarithms will be taken to the base e.

transmitted. If P_{ei} is the probability that the decoder makes an incorrect choice when code word i is transmitted ($i = 1, 2, 3, \cdots, M$), and if each of the M code words is equally likely to be transmitted, then the overall probability of a decoding error is

$$P_e = (1/M)\sum_{i=1} P_{ei}. \tag{9}$$

The optimal decoder is defined as the decoding system which minimizes P_e for a given code.

As was done for the binary symmetric channel in Section I we shall consider two types of decoding.

Channel A: The optimal decoder may be shown to be the one which selects that code word $\mathbf{x}$ which minimizes the Hamming distance, $d_H(\mathbf{x},\mathbf{y})$ between $\mathbf{x}$ and the received vector $\mathbf{y}$. Accordingly, we define the "discrepancy" as the Hamming distance, and the optimal decoder is the *minimum discrepancy decoder* (or *minimum distance decoder*) denoted by MDD. Let us denote by P_{eM} the probability of error (P_e) using MDD.

The channel capacity of Channel A is readily shown to be

$$C = C(p_o) = \ln q - H(p_o) - p_o \ln (q - 1), \tag{10}$$

where

$$H(\rho) = -\rho \ln \rho - (1 - \rho) \ln (1 - \rho). \tag{11}$$

The Fundamental Theorem of Information Theory[1,7] states that for any $R < C$ there exists a sequence of n-dimensional codes (one for each n) such that $P_{eM} = e^{-nE(R)+o(n)}$ (where $E(R) > 0$ when $R < C$). Further if $R > C$, $P_{eM} \xrightarrow{n} 1$ so that C is the supremum of those rates for which it is possible to obtain vanishingly small error probability using MDD.

The second type of decoding is described as follows: For the code being used, let d be the minimum Hamming distance between pairs of code words. About each of the M code words we construct a "sphere" in the space of q^n n-vectors, consisting of those vectors not more than Hamming distance $(d - 1)/2$ from that code word. All these spheres are disjoint. If the received vector is in the sphere about code word i, it is decoded as code word i. If the received vector is in no sphere, then the decoder announces an error. We term this type of decoding *bounded discrepancy decoding* (BDD), and denote the resulting error probability by P_{eB}. (i.e., P_{eB} is the probability that the received vector is not in the sphere about the transmitted code word.) Alternately, the bounded discrepancy decoder corrects errors affecting up to $e = (d - 1)/2$ positions and no more. Clearly $P_{eB} \geqq P_{eM}$.

In connection with BDD we are interested in the quantity $M(n,d)$, the maximum number of code words in an n-dimensional code with minimum distance d. The corresponding transmission rate is $R(n,d) = (1/n) \ln M(n,d)$. The following bounds hold:

For $d/2n > (q-1)/2q$:

$$M(n,d) \leqq \frac{\beta}{\beta - \left(\frac{q-1}{2q}\right)}. \tag{12a}$$

For $d/2n < (q-1)/2q$:

$$\frac{q^n}{\sum_{r=0}^{d-2} \binom{n}{r} (q-1)^r} \leqq M(n,d) \leqq \begin{cases} q^{n[1-(2q/q-1)\beta]} qd \\ \dfrac{nq^n K(\beta)}{\sum_{r=0}^{[td/2]} \binom{n}{r} (q-1)^r \left(\frac{td}{2} - r\right)} \end{cases}, \tag{12b}$$

where

$$\beta = d/2n, \tag{12c}$$

$$t = \frac{q-1}{q\beta}\left[1 - \sqrt{1 - \frac{2q}{q-1}\beta}\right], \tag{12d}$$

$$K(\beta) = \beta/[1 - t\beta q/(q-1)], \tag{12e}$$

and where $[x]$ denotes the largest integer not greater than x. The upper bound (12a) and the first upper bound of (12b) are the well known Plotkin bounds,[8,9] and the lower bound of (12b) is the well known Varshamov-Gilbert-Sacks bound as given in Ref. 8; the second upper bound of (12b) is established in Section III.

Now let us let n and d become large while the ratio $\beta = d/2n$ is held fixed, and define $R(\beta) = \lim_{n\to\infty} R(n,d) = \lim_{n\to\infty} R(n,2\beta n)$. We obtain from (12a):

$$R(\beta) = 0, \qquad \beta > (q-1)/2q, \tag{13a}$$

and from (12b):

$$\ln q - H(2\beta) - 2\beta \ln (q-1) \leqq R(\beta) \leqq \begin{cases} \left(1 - \dfrac{2q\beta}{q-1}\right) \ln q, \\ \ln q - H(t\beta) - t\beta \ln (q-1), \end{cases} \tag{13b}$$

where $H(\rho)$ is defined by (11). The second upper bound in (13b) is the same as the Elias bound[4] which was obtained independently. Although

the bounds of (12) and (13) are of interest in themselves, we make use of them here to demonstrate the following:

Theorem A: There exists a fixed rate C_B, called the "bounded discrepancy decoding channel capacity," such that for any rate $R < C_B$, there exists a sequence of n-dimensional codes (one for each n) such that $P_{eB} = \exp [-nE_B(R) + o(n)]$ (where $E_B(R) > 0$ for $R < C_B$). Further if $R > C_B$, $P_{eB} \xrightarrow{n} 1$, so that C_B is the supremum of those rates for which it is possible to obtain vanishingly small error probability using BDD.

For channel A we shall show

$$C(2p_o) \leqq C_B \leqq C(tp_o) < C(p_o) = C, \tag{14}$$

so that C_B is strictly less than C the "maximum error free" rate using MDD.

Finally we can estimate $E_B(R)$ by

$$\alpha\left(\frac{s}{2}, p_o\right) \leqq E_B(R) \leqq \begin{cases} \alpha\left(s\left[1 - \dfrac{q}{2(q-1)}\, s\right], p_o\right), \\ \alpha\left(\dfrac{q-1}{2q}\left[\dfrac{H(s) + s \ln (q-1)}{\ln q}\right], p_o\right), \end{cases} \tag{15}$$

where $s = s(R)$ is defined by

$$R = C(s) = \ln q - H(s) - s \ln (q-1), \tag{15a}$$

and

$$\alpha(\rho, p_o) = \rho \ln \frac{\rho}{p_o} + (1-\rho) \ln \frac{(1-\rho)}{(1-p_o)}. \tag{15b}$$

Channel B: For this channel it may be shown that the optimum decoder minimizes the Euclidean distance $d_E(\mathbf{x},\mathbf{y})$ between the received vector $\mathbf{y}$ and the code word $\mathbf{x}$. Accordingly, we define the discrepancy as the Euclidean distance d_E, so that the optimal decoder is the minimum discrepancy decoder (MDD). Here too the channel capacity C is the maximum rate below which it is possible to obtain vanishingly small P_{eM}. An exact expression for C is not known but it has been estimated by upper and lower bounds by Shannon[1] and a method for computing C is outlined by Wolfowitz.[10] Bounded discrepancy decoding (BDD) is defined exactly as for Channel A with the Euclidean distance used instead of the Hamming distance.

Let $M(n,d^2)$ be the maximum number of points in an n-dimensional code with minimum distance d, and let $R(n,d^2) = (1/n) \ln M(n,d^2)$ be

the corresponding transmission rate. We let n and d become large while the ratio $\beta = (d/2)^2/n = d^2/(4n)$ is held fixed, and define $R(\beta) = \lim_{n\to\infty} R(n,d^2) = \lim_{n\to\infty} R(n,4\beta n)$. Let $\hat{\beta} = \beta/A^2$. The following estimate of $R(\beta)$ is obtained:

$$R_L(\beta) \leqq R(\beta) \leqq R_U(\beta) \tag{16}$$

where

$$R_U(\beta) = \begin{cases} 0 & \hat{\beta} \geqq \frac{1}{2} \\ (2 \ln 2)(1 - 2\hat{\beta}), & \frac{1}{4} \leqq \hat{\beta} < \frac{1}{2} \\ \dfrac{k^2}{k^2 - 2} \ln k(1 - 2\hat{\beta}), & \dfrac{1}{k^2} \leqq \hat{\beta} < \dfrac{1}{(k-1)^2} \\ & (k = 3, 4, 5, \cdots) \end{cases} \tag{17}$$

and

$$R_L(\beta) = \max \begin{cases} \ln 2 + \hat{\beta} \ln (\hat{\beta}) + (1 - \hat{\beta}) \ln (1 - \hat{\beta}) = R_{L1} \\ C_o(4\beta) = R_{L2} \end{cases} \tag{18}$$

where $C_o(\xi)$ is defined by

$$C_o(\xi) = \ln 2AK_o(\xi) - \xi\lambda(\xi), \tag{19}$$

and where $\lambda(\xi)$ is defined by

$$\int_0^A r(u) e^{-\lambda(\xi) r(u)} du = \xi \int_0^A e^{-\lambda(\xi) r(u)} du, \tag{19a}$$

where

$$r(u) = u^2, \tag{19b}$$

and

$$K(\xi) = \left[\int_{-A}^{A} e^{-\lambda(\xi) r(u)} du \right]^{-1}. \tag{19c}$$

It is verified in Appendix A tbat for $0 < \xi/A^2 \leqq \frac{1}{3}$, there exists a unique $\lambda(\xi)$ satisfying (19a). The first value of the lower bound R_{L1} is dominant for $0.02 \leqq \hat{\beta} < 0.5$, and the second R_{L2} for $0 < \hat{\beta} \leqq 0.02$.

We make use of the estimate of $R(\beta)$ (16) to establish Theorem A for Channel B. Here we have

$$R_L(N) \leqq C_B \leqq R_U(N). \tag{20}$$

For large values of A^2/N,

$$C_B \geqq C - \ln 2 + \epsilon(A^2/N), \tag{21}$$

where C is the channel capacity, the maximum "error free" rate using MDD, and $\epsilon \to 0$ as $A^2/N \to \infty$. Thus for large values of the "signal-to-noise ratio" A^2/N, C_B is within a constant of C, so that the ratio $C_B/C \to 1$ as $A^2/N \to \infty$. An estimate of $E_B(R)$ is also obtained.

Channel C: As with Channel B, the optimal decoder is the decoder which selects that code word $\mathbf{x}$ which has the smallest Euclidean distance from the received vector $\mathbf{y}$. Thus if $\mathbf{y} = (y_1, y_2, \cdots, y_n)$, the decoder announces that code word $\mathbf{x}$ which minimizes (with respect to $\mathbf{x}$)

$$d_E(\mathbf{x},\mathbf{y}) = \sum_{k=1}^{n} (x_k - y_k)^2 = \sum_k x_k^2 + \sum_k y_k^2 - 2\sum_k x_k y_k . \tag{22}$$

Since $\sum_k x_k^2 = nP$, $d_E(\mathbf{x},\mathbf{y})$ is minimized when $\sum_k x_k y_k$ is maximized. Hence optimal decoding is equivalent to selection of that code word $\mathbf{x}$ which minimizes the angle $a(\mathbf{x},\mathbf{y})$ between $\mathbf{x}$ and $\mathbf{y}$, where

$$\cos a(\mathbf{x},\mathbf{y}) = \frac{\sum_k x_k y_k}{\left[\sum_k x_k^2 \cdot \sum_k y_k^2\right]^{\frac{1}{2}}}. \tag{23}$$

Thus if we define the discrepancy between $\mathbf{x}$ and $\mathbf{y}$ as the angle $a(\mathbf{x},\mathbf{y})$, the optimal decoder is the minimum discrepancy decoder (MDD). Let us denote by P_{eM} the error probability using MDD.

The channel capacity is $C = \frac{1}{2} \ln [1 + (P/N)]$, and is the maximum rate below which it is possible to obtain vanishingly small P_{eM}. Further for any $R < C$, there exists a sequence of n-dimensional codes such that $P_{eM} = e^{-nE(R)+o(n)}$. Estimates of $E(R)$ are obtained in Refs. 11 and 12.

The bounded discrepancy decoder (and P_{eB}) is defined exactly as for Channels A and B but with the angle $a(\mathbf{x},\mathbf{y})$ used instead of the Hamming or the Euclidean distance.

In connection with BDD we consider $M(n,\theta)$, the maximum number of points in an n-dimensional code with minimum angle θ, and the corresponding rate $R(n,\theta) = (1/n) \ln M(n,\theta)$. The following bounds hold for $\theta < \pi/2$:

$$\frac{n}{n-1}\sqrt{\pi}\,\frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n+2}{2}\right)}\left[\int_0^{\theta} \sin^{n-2}\varphi\, d\varphi\right]^{-1}$$

$$\leqq M(n,\theta) \tag{24}$$

$$\leqq \frac{\sqrt{\pi}\,\Gamma\left(\frac{n-1}{2}\right)\sin\psi\,\tan\psi}{2\Gamma\left(\frac{n}{2}\right)\int_0^{\psi}(\sin\varphi)^{n-2}\,(\cos\varphi-\cos\psi)\,d\varphi}$$

where $\psi = \sin^{-1}\sqrt{2}\,\sin(\theta/2)$. The upper bound was obtained by Rankin,[13] and the lower bound is obtained in Section V. If we let n become large while θ is held fixed and let $R(\theta) = \lim_{n\to\infty} R(n,\theta)$ we can obtain from (24)

$$-\ln\sin\theta \leqq R(\theta) \leqq -\ln\sqrt{2}\,\sin(\theta/2). \tag{25}$$

Inequalities (25) will be used to establish Theorem A for Channel C. Here we have

$$C - \ln 2 - \tfrac{1}{2}\ln(1-e^{-2C}) \leqq C_B \leqq C - \tfrac{1}{2}\ln 2. \tag{26}$$

Estimates will also be obtained for the exponent $E_B(R)$ and comparisons to the estimates of $E(R)$ will be made.

Channel D: For this channel we shall find the optimal decoding scheme by proceding as follows. Define the function $r(u)$ by

$$r(u) = \frac{1}{\lambda}\ln\frac{p(0)}{p(u)}, \qquad -A \leqq u \leqq +A \tag{27}$$

where $p(u)$ is the noise probability density function which satisfies assumptions (8), and λ is a constant to be specified later. Equation (27) is meaningful since by (8b), $p(u) \neq 0$. From (27) we see that

$$p(u) = p(0)\exp[-\lambda r(u)] = K_o\exp[-\lambda r(u)], \tag{28}$$

where $K_o = p(0)$. The n-fold joint probability density for the n independent noise coordinates is

$$p_n(u_1, u_2, \cdots, u_n) = \prod_{k=1}^{n} p(u_k) = K_o{}^n\exp\left[-\lambda\sum_{k=1}^{n} r(u_k)\right]. \tag{29}$$

Let us now consider the decoder. Suppose that the received vector is $\mathbf{y}$. It is not hard to show that the probability of incorrect decoding is minimized when the decoder selects that code word $\mathbf{x}$ which maximizes $p(\mathbf{y}|\mathbf{x})$, the conditional probability density of receiving $\mathbf{y}$ given that $\mathbf{x}$ is transmitted. This quantity is

$$p(\mathbf{y} \mid \mathbf{x}) = p_n(y_1 \dot{-} x_1, y_2 \dot{-} x_2, \cdots, y_n \dot{-} x_n) = K_o^n \exp\left[-\lambda \sum_{k=1}^{n} r(y_k \dot{-} x_k)\right]. \tag{30}$$

The subtraction of coordinates $y_k \dot{-} x_k$ in (30) is performed modulo $2A$ with the result reduced into the interval $[-A,+A]$. Thus for a given $\mathbf{y}$, the optimal decoder selects that code word $\mathbf{x}$ which minimizes

$$d_o(\mathbf{x},\mathbf{y}) = \sum_{k=1}^{n} r(y_k \dot{-} x_k). \tag{31}$$

The function $d_o(\mathbf{x},\mathbf{y})$ defined on $\mathcal{C}_n \times \mathcal{C}_n$ will be defined as the discrepancy function, so that the optimal decoder is the minimum discrepancy decoder (MDD). Denote the resulting error probability by P_{eM}.

Let us remark at this point that the discrepancy has the following properties:

(a) $d_o(\mathbf{x},\mathbf{y}) \geqq 0$, with equality if and only if $\mathbf{x} = \mathbf{y}$.
(b) $d_o(\mathbf{x},\mathbf{y}) = d_o(\mathbf{y},\mathbf{x})$.

It is not necessarily a metric, however, since the triangle inequality need not hold.

For any vector $\boldsymbol{\alpha} \in \mathcal{C}_n$, let the "region" $S_n(\boldsymbol{\alpha},\rho)$ be the set of vectors $\boldsymbol{\beta} \in \mathcal{C}_n$ satisfying $d_o(\boldsymbol{\alpha},\boldsymbol{\beta}) < \rho$. We say that a code has *discrepancy* ρ if the regions $S_n(\mathbf{x},\rho)$ about all M code words $\mathbf{x}$ are disjoint.

We now describe another, though nonoptimum decoding technique. Let ρ_o be the largest number such that the code under consideration has discrepancy ρ_o. Hence the regions $S_n(\mathbf{x},\rho_o)$ for all code words $\mathbf{x}$ are disjoint. If the received vector $\mathbf{y} \in S_n(\mathbf{x},\rho_o)$ for some code word $\mathbf{x}$, then it is decoded as $\mathbf{x}$. If $\mathbf{y}$ belongs to no region, an error is announced. We term this type of decoding bounded discrepancy decoding (BDD), and denote the resulting error probability by P_{eB}. Clearly $P_{eB} \geqq P_{eM}$.

A case of special interest is that for which $p(u) = K_o \exp(-\lambda u^2)$. This channel is similar to channel B when λ is large (so that the effects of wrapping the interval $[-A,+A]$ onto a circle are minimized]. In this case $r(u) = u^2$.

Suppose we are given a function $r(u)$ defined on $[-A,+A]$. This function defines a discrepancy which is appropriate for the class of noise densities $p(u) = K_o \exp[-\lambda r(u)]$. Now a given member of the class could be specified by the parameter λ. (K_o is then determined by setting the total mass of $p(u)$ equal to unity.) It is convenient instead to specify a given member of the class by the parameter N defined by

$$N = E[r(z)] = \int_{-A}^{+A} r(u)\,p(u)\,du = \int_{-A}^{+A} r(u)\,K_o e^{-\lambda r(u)}\,du. \quad (32)$$

That is, given the parameter N corresponding to a $\lambda \geqq 0$, and the function $r(u)$, one can solve (32) for λ and K_o. Thus $r(u)$ and N specify the channel. For example if $r(u) = u^2$, then $N = E[z^2]$ is the average noise "power." It is shown in Appendix H that the channel capacity, the maximum "error free" rate using MDD is

$$C = C_o(N) \quad (33)$$

where the function $C_o(\xi)$ is defined by (19) with the appropriate function $r(u)$. It is shown in Appendix A, that $C_o(\xi)$ is well defined for

$$0 < \xi \leqq \frac{1}{A}\int_0^A r(u)\,du.$$

Let us now consider BDD. Two important quantities here are $M(n,\rho)$ the largest number of code points in an n-dimensional code with discrepancy ρ, and the corresponding rate $R(n,\rho) = (1/n)\ln M(n,\rho)$. We let n and ρ become large while the ratio $\beta = \rho/n$ is held fixed, and then define $R(\beta) = \lim_{n\to\infty} R(n,\rho) = \lim_{n\to\infty} R(n,\beta n)$. It is shown in Section VI that

$$C_o(2\eta\beta) \leqq R(\beta) \leqq C_o(\beta), \quad (34)$$

where $C_o(\xi)$ is defined by (19), and η is defined by

$$\eta = \sup_{-A\leqq u_1,u_2\leqq +A} \frac{r(u_1 \dotplus u_2)}{r(u_1) + r(u_2)}. \quad (35)$$

The addition in (35), $u_1 \dotplus u_2$, is modulo $2A$, with the result reduced into the interval $[-A,+A]$. It is shown in Appendix B that η is finite.

The estimate (34) of $R(\beta)$ is used to establish Theorem A for channel D. Here C_B can be estimated by

$$C_o(2\eta N) \leqq C_B \leqq C_o(N) = C. \quad (36)$$

For the special case of the quadratic discrepancy $r(u) = u^2$, the quantity $\eta = 2$, so that the left-hand member of (36) is $C(4N)$. It will be shown that in this case C_B is bounded above by $C_o(2N)$ so that

$$C_o(4N) \leqq C_B \leqq C_o(2N) < C_o(N) = C. \quad (37)$$

Hence in this case C_B is strictly less than C. Further, both the upper and lower bounds of (37) will be refined for small values of the "signal-to-noise" ratio A^2/N.

For large values of "signal-to-noise ratio" A^2/N, (37) becomes

$$\frac{1}{2}\ln\frac{1}{2\pi e}\frac{A^2}{N}+\epsilon_1\left(\frac{A^2}{N}\right)\leqq C_B\leqq\frac{1}{2}\ln\frac{1}{\pi e}\frac{A^2}{N}+\epsilon_2\left(\frac{A^2}{N}\right),\qquad(38)$$

where ϵ_1, $\epsilon_2\to 0$ as $A^2/N\to\infty$. It will follow that C_B is within a constant of C, so that the ratio $C_B/C\to 1$ as $A^2/N\to\infty$.

III. CHANNEL A (DISCRETE CHANNEL):

3.1 *Lower Bound on $M(n,d)$*

Our first task is to obtain the second upper bound on $M(n,d)$ of inequality (12b). We need the following lemmas:

Lemma 3.1: Let $g_1, g_2, \cdots, g_n$ be real numbers. Then

$$\sum_{k=1}^{n} g_k^2\geqq\frac{1}{n}\left(\sum g_k\right)^2.\qquad(39)$$

Proof: From the Schwarz inequality

$$\left(\sum_{k=1}^{n}1\cdot g_k\right)^2\leqq\left(\sum_{k=1}^{n}1^2\right)\left(\sum_{k=1}^{n}g_k^2\right)=n\sum_{k=1}^{n}g_k^2.$$

Lemma 3.2: Given a code with minimum distance d, let $\mathbf{x}_i=(x_{i1}, x_{i2}, \cdots, x_{in})$, $i=1, 2, \cdots, m$ be any set of m points from the code. Let $\mathbf{z}$ be any n-vector and r_i $(i=1, 2, \cdots, m)$ the Hamming distance $d_H(\mathbf{x}_i, \mathbf{z})$ from $\mathbf{x}_i$ to $\mathbf{z}$. Then

$$\left(\frac{\sum_{i=1}^{m}r_i}{n}\right)^2-\frac{2(q-1)m}{q}\left(\frac{\sum_{i=1}^{m}r_i}{n}\right)+\frac{(q-1)}{q}m(m-1)\frac{d}{n}\leqq 0.\qquad(40)$$

Proof: Without loss of generality assume $\mathbf{z}=0$. Arrange the m code words in an array

$$\begin{aligned}\mathbf{x}_1&=x_{11}, x_{12}, \cdots, x_{1n}\\&\vdots\\\mathbf{x}_m&=x_{m1}, x_{m2}, \cdots, x_{mn}.\end{aligned}$$

Denote by s_{jk} $(j=0, 1, \cdots, q-1;\ k=1, 2, \cdots, n)$ the number of times symbol j appears in column k. Then, since the code has minimum distance d,

$$\binom{m}{2}d\leqq\sum_{1\leqq r<i\leqq m}d_H(\mathbf{x}_r, \mathbf{x}_i)=\sum_{k=1}^{n}\sum_{j=0}^{q-1}\tfrac{1}{2}s_{jk}(m-s_{jk})$$

$$= \sum_k \sum_j \tfrac{1}{2} m s_{jk} - \sum_k \sum_j \tfrac{1}{2} s_{jk}^2.$$

Now $\sum_k \sum_j s_{jk} = mn$ so that

$$\binom{m}{2} d \leqq \frac{m^2 n}{2} - \frac{1}{2} \sum_k s_{0k}^2 - \frac{1}{2} \sum_k \sum_{j>0} s_{jk}^2. \tag{41}$$

Since $s_{0k} = m - \sum_{j>0} s_{jk}$, by Lemma 3.1,

$$\sum_k s_{0k}^2 \leqq \frac{1}{n} \left[\sum_{k=1}^{n} \left(m - \sum_{j>0} s_{jk} \right) \right]^2 = \frac{1}{n} \left[mn - \sum_k \sum_{j>0} s_{jk} \right]^2. \tag{42}$$

Also by Lemma 3.1,

$$\sum_{k=1}^{n} \sum_{j=1}^{q-1} s_{jk}^2 \geqq \frac{1}{(q-1)n} \left[\sum_k \sum_{j>0} s_{jk} \right]^2. \tag{43}$$

Observing that $\sum_k \sum_{j>0} s_{jk} = \sum_{i=1}^{m} r_i$, and substituting (42) and (43) into (41), we obtain

$$\begin{aligned} \binom{m}{2} d &\leqq \frac{m^2 n}{2} - \frac{1}{2n} (nm - \sum_i r_i)^2 \\ &\quad - \frac{1}{2n(q-1)} (\sum_i r_i)^2 = m \sum_i r_i - \frac{q}{2(q-1)n} (\sum_i r_i)^2. \end{aligned} \tag{44}$$

On dividing (44) by $nq/2(q-1)$, the lemma follows.

Derivation of the Bound:

Let us assume that we have an n-dimensional code with minimum distance $d(d/2n < (q-1)/2q)$ with $M = M(n,d)$ code points. Consider the "sphere" of radius $t(d/2)$ in the space of n-vectors about each code point where

$$t = \frac{q-1}{q\beta} \left(1 - \sqrt{1 - \frac{2q}{(q-1)} \beta} \right) \tag{45}$$

and $\beta = d/2n$. (Since $t \geqq 1$, these spheres are not necessarily disjoint.) To each point of the sphere at Hamming distance r from the center assign weight $\omega(r) = td/2 - r$. The "mass" μ of each sphere is therefore

$$\mu = \sum_{r=0}^{\lfloor td/2 \rfloor} \binom{n}{r} (q-1)^r \left(\frac{td}{2} - r \right). \tag{46}$$

If an n-vector $\mathbf{z}$ is simultaneously in the sphere about the m code words $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_m$, then we assign a weight $\omega_{\mathbf{z}}$ to $\mathbf{z}$ given by the sum of its weights in each sphere, i.e.,

$$\omega_{\mathbf{z}} = \sum_{i=1}^{m} \omega(r_i) = \frac{mtd}{2} - \sum_{i=1}^{m} r_i, \tag{47}$$

where $r_i = d_H(\mathbf{x}_i, \mathbf{z})$. If $\mathbf{z}$ lies in no sphere $\omega_{\mathbf{z}} = 0$. Consequently, we have

$$\text{mass of all } n\text{-vectors} = \sum_{\substack{\text{all } n\text{-vectors} \\ \mathbf{z}}} \omega_{\mathbf{z}} = M(n,d) \cdot \mu. \tag{48}$$

We will bound M by finding a bound on $\sum \omega_{\mathbf{z}}$. Letting $s = s_{\mathbf{z}} = \omega_{\mathbf{z}}/n$, (47) becomes

$$\frac{\sum_i r_i}{n} = \frac{mtd}{2n} - s = mt\beta - s. \tag{49}$$

Substituting (49) into (40) we get

$$\begin{aligned} m^2t^2\beta^2 - 2mt\beta s + s^2 - 2\frac{(q-1)}{q} m^2t\beta \\ + 2\frac{(q-1)}{q} ms + 2\frac{(q-1)}{q} m^2\beta - \frac{2(q-1)}{q} \beta m \leqq 0. \end{aligned} \tag{50}$$

Rewriting (50)

$$\begin{aligned} 0 \leqq s^2 \leqq m \Bigg[& 2\frac{(q-1)}{q} \beta \\ & - m\beta \left(t^2\beta - 2\frac{(q-1)}{q} t + 2\frac{(q-1)}{q} \right) \\ & - s\left(2\frac{(q-1)}{q} - 2t\beta \right) \Bigg]. \end{aligned} \tag{51}$$

Since by choice of t (45),

$$t^2\beta - 2\frac{(q-1)}{q} t + 2\frac{(q-1)}{q} = 0,$$

and

$$2\frac{(q-1)}{q} - 2\beta t > 0 \quad \text{when} \quad \beta < \frac{q-1}{2q},$$

(51) can be satisfied only when

$$s \leqq \frac{\beta}{1 - t\beta q/(q-1)} \triangleq K(\beta). \tag{52}$$

Thus

$$\sum_{\substack{\text{all } n\text{-vectors} \\ \mathbf{z}}} \omega_{\mathbf{z}} = \sum s \cdot n \leqq K(\beta) n q^n. \tag{53}$$

Hence from (53), (48) and (46) we have

$$M(n,d) \leqq \frac{K(\beta) n q^n}{\sum_{r=0}^{[t\beta n]} \binom{n}{r} (t\beta n - r)(q-1)^r}, \tag{54}$$

where

$$t = \frac{q-1}{q\beta}\left(1 - \sqrt{1 - \frac{2q\beta}{q-1}}\right), \qquad K(\beta) = \frac{\beta}{1 - t\beta q/(q-1)},$$

and $\beta < (q-1)/2q$.

3.2 *Asymptotic Estimates of $M(n,d)$ (13)*

Equation (13a) and the first upper bound of (13b) follow directly from (12a) and the first upper bound of (12b) by writing $R(n,2\beta n) = (1/n) \ln M(n,2\beta n)$ and letting n tend to infinity. The lower bound on $R(\beta)$ of (13b) follows from the lower bound on $M(n,d)$ of (12b) and the fact that (Ref. 8, Appendix A)

$$\lim_{n\to\infty} \frac{1}{n} \ln \sum_{r=0}^{\xi n} \binom{n}{r} (q-1)^r = H(\xi) - \xi \ln (q-1). \tag{55}$$

The second upper bound of (13b) follows from (54) and (55) and the fact that

$$\sum_{r=0}^{[t\beta n]} \binom{n}{r} \left(\frac{td}{2} - r\right) (q-1)^r \geqq \sum_{r=0}^{[t\beta n]-1} \binom{n}{r} (q-1)^r. \tag{56}$$

In the important special case of binary codes ($q = 2$), the second upper bound of (13b) is always sharper than the first upper bound. Thus for $q = 2$ we have for $\beta < \frac{1}{4}$:

$$1 - H(2\beta) \leqq R(\beta) \leqq 1 - H\left(\tfrac{1}{2} - \tfrac{1}{2}\sqrt{1 - 4\beta}\right). \tag{57}$$

These upper and lower bounds converge at $\beta = \frac{1}{4}$ yielding $R(\beta) = 0$, $\beta \geqq \frac{1}{4}$. Inequality (57), is plotted in Fig. 2.

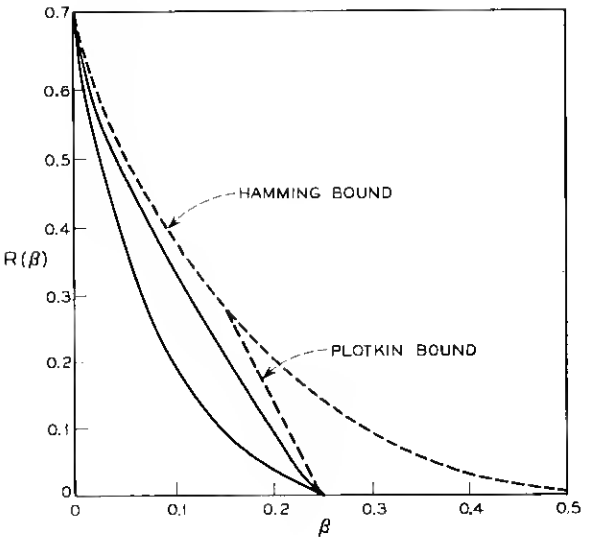

Fig. 2 (Channel A) — Upper and lower bounds on $R(\beta)$ for the binary symmetric channel (57). The dotted lines are the best bounds given in Ref. 8.

3.3 *Bounded Discrepancy Decoding Channel Capacity*

When Shannon's Fundamental Coding Theorem is applied to channel A, one finds that for every R less than the channel capacity $C = 1 - H(p_o) - p_o \ln (q - 1)$, there exists a sequence of codes (one for each n) with transmission rate R such that the error probability using MDD, $P_{eM} \overset{n}{\to} 0$. Further $R > C$, $P_{eM} \overset{n}{\to} 1$. Thus the channel capacity C is the supremum of those rates R for which it is possible (asymptotically in n) to obtain vanishingly small error probability using (optimal) MDD. We now ask what is the largest rate for which it is possible to obtain asymptotically vanishingly small error probability using BDD?

Let us suppose that for every n, an n-dimensional code is available with $d/2n = \beta$. Using BDD we have error probability

$$P_{eB} = \Pr [\text{number of errors} \geqq d/2 = \beta n]. \tag{58}$$

Since the errors in each digit occur independently with probability p_o, we have by the weak law of large numbers that $\lim_{n\to\infty} P_{eB} = 0$ or 1 according as $\beta > p_o$ or $\beta < p_o$.

If we define the *bounded discrepancy decoding channel capacity*, de-

noted by C_B, as the supremum of the rates for which it is possible (asymptotically in n) to obtain vanishingly small P_{eB}, we have from the foregoing that $C_B = R(p_o)$. Making use of the second upper bound on $R(\beta)$ of (13b) and the fact that $t > 1$ for $\beta > 0$, we have for $p_o > 0$

$$C_B = R(p_o) \leqq 1 - H(tp_o) - tp_o \ln (q-1) = C(tp_o) < C. \quad (59)$$

Thus C_B is bounded away from C.

In the binary case ($q = 2$), we make use of (13b) or (57) to obtain

$$1 - H(2p_o) \leqq C_B \leqq 1 - H(\tfrac{1}{2} - \tfrac{1}{2}\sqrt{1 - 4p_o}). \quad (60)$$

Inequality (60) is plotted in Fig. 1.

3.4 *Exponential Behavior of P_{eB}*

For a fixed $R < C_B$, denote by P_{eB}^* the smallest attainable value of P_{eB}. It was shown above that $P_{eB}^* \xrightarrow{n} 0$. We shall now show that $P_{eB}^* = e^{-nE_B(R)+o(n)}$, where $E_B > 0$ and obtain estimates of $E_B(R)$.

Given an n and R, denote by $\beta_n(R)$ the largest value of β attainable for an n-dimensional code with transmission rate R. With R held fixed, let $\beta(R) = \lim_{n\to\infty} \beta_n(R)$. Then $\beta(R)$ satisfies

$$R_L(\beta(R)) \leqq R \leqq R_U(\beta(R)), \quad (61)$$

where $R_L(\beta)$ and $R_U(\beta)$ are the upper and lower bounds of (13b). If we define the parameter $s = s(R)$ by

$$R = \ln q - H(s) - s \ln (q-1), \quad (62)$$

we obtain from (61) and (13b)

$$\frac{s}{2} \leqq \beta(R) \leqq \begin{cases} \dfrac{q-1}{2q}\left[\dfrac{H(s) + s\ln(q-1)}{\ln q}\right] \\ s\left(1 - \dfrac{qs}{2(q-1)}\right). \end{cases} \quad (63)$$

Thus for any R there exists a code (for n sufficiently large) with minimum distance $d = \beta(R)\cdot 2n$. With R fixed, this code minimizes P_{eB}. Thus from (58)

$$P_{eB}^* = \Pr[\text{no. of errors} \geqq n\beta(R)]$$
$$= \sum_{r=[\beta(R)n]}^{n} \binom{n}{r} p_o^r (1-p_o)^{n-r}. \quad (64)$$

Making use of the fact that (Ref. 8, Appendix A)

$$\lim_{n\to\infty} -\frac{1}{n} \ln \sum_{r=\rho n}^{n} \binom{n}{r} p_o^{\,r} (1 - p_o)^{n-r} = \alpha(\rho,p_o), \tag{65}$$

where $\alpha(\rho,p_o) = \rho \ln (\rho/p_o) + (1 - \rho) \ln [(1 - \rho)/(1 - p_o)]$, we have from (64):

$$E_B(R) = -\lim_{n\to\infty} (1/n)\, P_{eB}{}^{*} = \alpha(\beta(R),p_o). \tag{66}$$

Inequality (63) provides bounds on $\beta(R)$ and hence an estimate of $E_B(R)$. Let us observe that for $R = 0$ $(s = (q - 1)/q)$ the upper and lower bounds on $\beta(R)$ (63) converge yielding $\beta(R) = (q - 1)/2q$ so that

$$E_B(0) = \alpha\left(\frac{q - 1}{2q}, p_o\right). \tag{67}$$

Further since $\alpha(p_o, p_o) = 0$, $E_B(R)$ vanishes when $R = R(p_o) = C_B$.

In the binary case, the second upper bound on $\beta(R)$ (63) is always sharper than the first, so that (66) yields

$$\alpha\left(\frac{s}{2}, p_o\right) \leqq E_B(R) \leqq \alpha(s(1 - s), p_o). \tag{68}$$

Inequality (68) is plotted in Figs. 3(a) and 3(b) for $p_o = 5 \times 10^{-2}$ and $p_o = 10^{-4}$ respectively. It can be seen from Fig. 3(b) that for certain values of R the upper bound on $E_B(R)$ is greater than the lower bound on $E(R)$ (the best exponent for MDD). Thus although $E \geqq E_B$ (since $P_{eM} \leqq P_{eB}$), there is nothing to indicate that the strict inequality always holds.

IV. CHANNEL B (GAUSSIAN CHANNEL WITH AMPLITUDE CONSTRAINT)

Our first task is to establish the bounds on $R(\beta)$ given in Section II.

4.1 *Lower Bound on* $R(\beta)$

4.1.1 *Bound for Large* β

It would not violate the code constraints if the coordinates of the code words were further restricted to be $\pm A$. In this case the code is a binary code and the Hamming distance $d_H(\mathbf{x},\mathbf{y})$ between two vectors $\mathbf{x}$ and $\mathbf{y}$ is related to the Euclidean distance $d_E(\mathbf{x},\mathbf{y})$ by

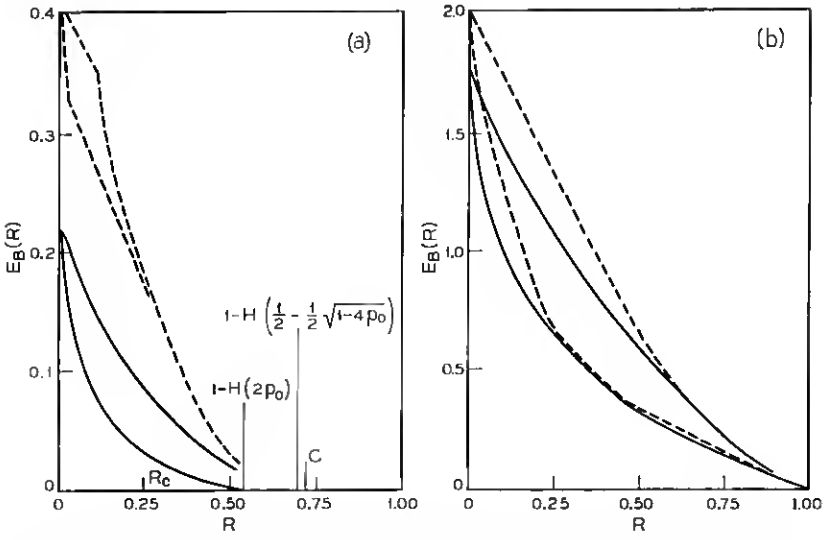

Fig. 3(a) (Channel A) — Upper and lower bounds on the exponent $E_B(R)$ for the case $q = 2$ with $p_o = 0.05$ (solid lines). Upper and lower bounds on $E(R)$ are in dotted lines.

Fig. 3(b) (Channel A) — Upper and lower bounds on the exponent $E_B(R)$ for the case $q = 2$ with $p_o = 10^{-4}$ (solid lines). Upper and lower bounds on $E(R)$ are in dotted lines.

$$d_H(\mathbf{x},\mathbf{y}) = d_E^2(\mathbf{x},\mathbf{y})/4A^2. \tag{69}$$

Thus if a code (with coordinates restricted to $\pm A$) has minimum Hamming distance $d_H = d/4A^2$, the minimum Euclidean distance is d. Thus $\hat{\beta} \triangleq \beta/A^2 = d/4A^2n = d_H/n$.

Now let $R_B(n,d_H)$ be the maximum rate for which a binary n-dimensional code with minimum Hamming distance d_H exists. We let n, and d_H become large while the ratio $\alpha = d_H/n$ is held fixed, and define $R_B(\alpha) = \lim_{n\to\infty} R_B(n,\alpha n)$. In the light of the above $R(\beta) \geqq R_B(\hat{\beta})$. The Gilbert bound (13b) (Ref. 8, p. 52) tells us that

$$R_B(\hat{\beta}) \geqq \ln 2 + \hat{\beta} \ln \hat{\beta} + (1 - \hat{\beta}) \ln (1 - \hat{\beta}) \text{ for } 0 \leqq \hat{\beta} \leqq \tfrac{1}{2}.$$

Thus we have

$$R(\beta) \geqq \ln 2 + \hat{\beta} \ln \hat{\beta} + (1 - \hat{\beta}) \ln (1 - \hat{\beta}) = R_{L_1}. \tag{70}$$

4.1.2 *Bound for Small β*

Consider a maximum size n-dimensional code with minimum distance d, and with $M = M(n,d^2)$ code points $\mathbf{x}_1, \cdots, \mathbf{x}_M$. About each code

point $\mathbf{x}_\mu$ construct an open hypersphere in n-space of radius d. Let V_μ denote the volume of the intersection of this sphere with the n-cube $[-A,+A]^n$. Now the union of these M spheres must cover the n-cube: for if $\mathbf{x}_o \in [-A,+A]^n$ is not contained in one of the spheres, $d(\mathbf{x}_o, \mathbf{x}_\nu) \geqq d$ for all ν, so that $\mathbf{x}_o$ may be added to the code destroying maximality. Thus

$$\sum_{\mu=1}^{M} V_\mu \geqq (2A)^n. \tag{71}$$

Now let S be the n-dimensional hypersphere of radius d with center at the origin, and $V_n(d)$ the volume of $S \cap [-A,+A]^n$. It is not hard to show that

$$V_\mu \leqq V_n(d), \qquad \mu = 1, 2, \cdots, M.$$

Consequently from (71)

$$MV_n(d) \geqq \sum_{\mu=1}^{M} V_\mu \geqq (2A)^n,$$

so that

$$M(n,d^2) \geqq [(2A)^n/V_n(d)]. \tag{72}$$

Applying the result of Appendix C to (72) yields

$$R(\beta) = \lim_{n\to\infty} (1/n) \ln M(n,4\beta n) \geqq C_o(4\beta). \tag{73}$$

It is shown in Appendix D that for small β

$$R_L(\beta) = R_{L_2}(\beta) = \tfrac{1}{2} \ln (A^2/2\pi e\beta) + \epsilon(\beta), \tag{74}$$

where $\epsilon(\beta) \to 0$ as $\beta \to 0$.

$R_L(\beta)$ is plotted in Figs. 4(a) and 4(b).

4.2 *Upper Bound on* $R(\beta)$

The approach used in this derivation is similar to Plotkin's technique for binary codes. We begin by obtaining the following:

Lemma 4.1: If $n < d^2/2A^2$ ($\hat{\beta} = d^2/4A^2n > \tfrac{1}{2}$),

$$M(n,d^2) \leqq \frac{d^2}{d^2 - 2A^2n} = \frac{2\hat{\beta}}{2\hat{\beta} - 1}. \tag{75}$$

Proof: Consider the maximum size n-dimensional code with minimum

distance d with $M = M(n,d^2)$ code points $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_M$. Let $\mathbf{x}_\nu = (x_{\nu 1}, x_{\nu 2}, \cdots, x_{\nu n})$. Then

$$\binom{M}{2} d^2 \leqq \sum_{1 \leqq \mu < \nu \leqq M} d^2(\mathbf{x}_\mu, \mathbf{x}_\nu) = \sum_{k=1}^{n} \sum_{\mu<\nu} (x_{\nu k} - x_{\mu k})^2$$

$$= \sum_{k=1}^{n} \left\{ M \sum_{\nu} x_{\nu k}^2 - \left(\sum_{\nu} x_{\nu k} \right)^2 \right\}$$

$$\leqq M \sum_{k=1}^{n} \sum_{\nu=1}^{M} x_{\nu k}^2 .$$

Since $x_{\nu k}^2 \leqq A^2$,

$$M(M-1)\frac{d^2}{2} = \binom{M}{2} d^2 \leqq M^2 n A^2 ,$$

from which

$$M(n,d^2)(d^2 - 2A^2 n) \leqq d^2,$$

and if $n < d^2/2A^2$,

$$M(n,d^2) \leqq \frac{d^2}{d^2 - 2A^2 n}, \tag{76}$$

completing the proof.

Lemma 4.2: Let α be an integer not less than two. Then

$$M(n,d) \leqq \alpha M[n-1, d^2 - (2A/\alpha)^2].$$

Proof: Again consider the maximum size code with $M(n,d)$ points. Partition the code into α classes $S_1, S_2, \cdots, S_\alpha$, where S_i consists of those code points $\mathbf{x}_\nu = (x_{\nu 1}, x_{\nu 2}, \cdots, x_{\nu n})$ such that

$$-A + (i-1)(2A/\alpha) \leqq x_{\nu 1} < -A + i(2A/\alpha), \qquad i = 1, 2, \cdots, \alpha.$$

In other words we partition the interval $[-A,+A]$ into α subintervals of length $2A/\alpha$, and assign $\mathbf{x}_\nu$ to class S_i according as its first coordinate $x_{\nu 1}$ is in the ith subinterval. (To be precise we must close the last subinterval ($i = \alpha$) at both ends to make the α subintervals cover $[-A,+A]$.)

Now delete the first coordinate from each point in the code. Each class S_i is now a code of length $n-1$ with minimum distance not less than

$$\sqrt{d^2 - \left(\frac{2A}{\alpha}\right)^2},$$

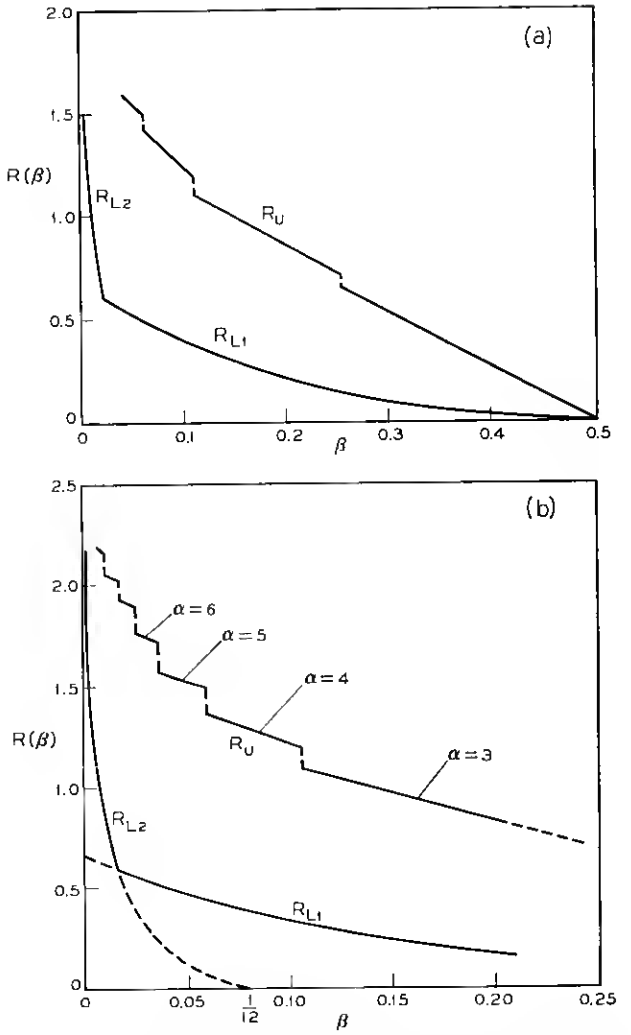

Fig. 4(a) (Channel B) — Upper and lower bounds on $R(\beta)$ vs β $(0 \leqq \beta \leqq 0.5)$.
Fig. 4(b) (Channel B) — Upper and lower bounds on $R(\beta)$ vs β $(0 \leqq \beta \leqq 0.2)$.

since the first coordinates of two code words in class S_i do not differ by more than $2A/\alpha$.

Further some class S_i has at least $M(n,d^2)/\alpha$ points, so that

$$M[n - 1, d^2 - (2A/\alpha)^2] \geqq (1/\alpha)\, M(n,d^2),$$

and the lemma follows.

Corollary: Let $a < (d\alpha/2A)^2$ *be an integer. Then*

$$M(n,d^2) \leqq \alpha^a M[n - a,\ d^2 - a(2A/\alpha)^2]. \tag{77}$$

Proof: Inequality (77) follows by repeated application of Lemma 4.2. Since by hypothesis $d^2 - a(2A/\alpha)^2 > 0$, the expression $M[n - a,\ d^2 - a(2A/\alpha)^2]$ is meaningful.

Derivation of the Bound

Let n_o be the greatest integer satisfying

$$n_o < \frac{1}{2A^2}\left[d^2 - (n - n_o)\left(\frac{2A}{\alpha}\right)^2\right], \tag{78}$$

where $\alpha \geqq 2$. Rearranging (78) we obtain

$$n_o < n\left[\frac{\alpha^2 \dfrac{d^2}{2A^2 n} - 2}{\alpha^2 - 2}\right] = n\left[\frac{2\hat{\beta}\alpha^2 - 2}{\alpha^2 - 2}\right]. \tag{79}$$

Let us also assume as an additional constraint on α that $\alpha^2 > 1/\hat{\beta}$, so that $[(2\hat{\beta}\alpha^2 - 2)/(\alpha^2 - 2)] > 0$, and for sufficiently large n, $n_o \geqq 1$. In fact for large n we may approximate n_o by

$$n_o = n\left[\frac{2\alpha^2\hat{\beta} - 2}{\alpha^2 - 2}\right]. \tag{80}$$

Now by choice of n_o (78), $0 < 2A^2 n_o < [d^2 - (n - n_o)(2A/\alpha)^2]$. Hence the Corollary to Lemma 4.2 applies with $a = n - n_o$ yielding

$$M(n,d^2) \leqq \alpha^{n-n_o} M[n_o\ ,\ d^2 - (n - n_o)(2A/\alpha^2)]. \tag{81}$$

Also by (78), we may apply Lemma 4.1 to get

$$M\left(n_o\ ,\ d^2 - (n - n_o)\left(\frac{2A}{\alpha^2}\right)^2\right)$$

$$\leqq \frac{d^2 - (n - n_o)\left(\dfrac{2A}{\alpha}\right)^2}{d^2 - (n - n_o)\left(\dfrac{2A}{\alpha}\right)^2 - 2A^2 n_o} \triangleq Q(\alpha,d,n). \tag{82}$$

Thus from (81) and (82) we have

$$M(n,d^2) \leqq \alpha^{n-n_o} Q(\alpha,d,n). \tag{83}$$

Taking logarithms yields:

$$R(n,d^2) \leqq \ln \alpha \left[1 - \frac{n_o}{n}\right] + \frac{1}{n} \ln Q(\alpha,d,n). \tag{84}$$

We now let n and d become large while holding the ratio $\hat{\beta} = d^2/4A^2n$ fixed. It is easy to show that

$$\frac{1}{n} \ln Q(\alpha, 2A\sqrt{\hat{\beta}n},n) \xrightarrow{n} 0, \tag{85}$$

so that using (80) we obtain

$$R(\beta) \leqq \ln \alpha \left[1 - \frac{2\hat{\beta}\alpha^2 - 2}{\alpha^2 - 2}\right] = [\ln \alpha]\left[\frac{\alpha^2}{\alpha^2 - 2}\right][1 - 2\hat{\beta}], \tag{86}$$

where α is an arbitrary integer satisfying $\alpha \geqq 2$, and $\alpha^2 > 1/\hat{\beta}$. Using the choice of α indicated in Appendix E we obtain $R(\beta) \leqq R_U(\beta)$ where

$$R_U(\beta) = \begin{cases} 2(\ln 2)(1 - 2\hat{\beta}), & \frac{1}{2} \geqq \beta \geqq \frac{1}{4} \\ \dfrac{k^2}{k^2 - 2}(\ln k)(1 - 2\hat{\beta}) & \dfrac{1}{(k-1)^2} > \hat{\beta} \geqq \dfrac{1}{k^2} \\ & (k = 3, 4, \cdots). \end{cases} \tag{87}$$

$R_U(\beta)$ is plotted in Figs. 4(a) and 4(b). For small values of $\hat{\beta}$, $\alpha \approx 1/\sqrt{\hat{\beta}}$ so we obtain

$$R_U(\beta) = -\tfrac{1}{2} \ln (\hat{\beta}) + \epsilon(\hat{\beta}), \tag{88}$$

where $\epsilon(\hat{\beta}) \to 0$ as $\hat{\beta} \to 0$.

4.3 *Bounded Discrepancy Decoding Channel Capacity*

Suppose that for every n, an n-dimensional code is available with $d^2/4n = \beta$. Using BDD we have error probability

$$P_{eB} = \Pr [d(\mathbf{x},\mathbf{y}) \geqq d/2] = \Pr [d^2(\mathbf{x},\mathbf{y}) \geqq \beta n]. \tag{89}$$

Since $d^2(\mathbf{x},\mathbf{y}) = \sum_{k=1}^{n} z_k^2$, where the z_k are the (normally distributed) noise components we have

$$P_{eB} = \Pr \left[\sum_{k=1}^{n} z^2/n \geqq \beta\right]. \tag{90}$$

By the weak law of large numbers $\sum z_i^2/n$ tends in probability to $N(= E(z_i^2))$. Thus $\lim_{n\to\infty} P_{eB} = 0$ or 1 according as $\beta > N$ or $\beta < N$.

We define the *bounded discrepancy decoding channel capacity* de-

noted by C_B as the supremum of the rates for which it is possible (asymptotically in n) to obtain vanishingly small error probability using BDD. From the foregoing we see that $C_B = R(N)$. Making use of the bounds on $R(\beta)$ established above we have

$$R_L(N) \leqq C_B \leqq R_U(N), \tag{91}$$

where R_L and R_U are defined by (17) and (18) respectively. These bounds on C_B are plotted vs the "signal-to-noise ratio" A^2/N in Fig. 5.

For large values of the ratio A^2/N (91) becomes [using (74) and (88)]

$$\frac{1}{2}\ln\frac{1}{2\pi e}\frac{A^2}{N} + \epsilon_1\left(\frac{A^2}{N}\right) \leqq C_B \leqq \frac{1}{2}\ln\frac{A^2}{N} + \epsilon_2\left(\frac{A^2}{N}\right) \tag{92}$$

where ϵ_1, $\epsilon_2 \to 0$ as $A^2/N \to \infty$.

The channel capacity is the "maximum error free rate" using MDD (clearly $C \geqq C_B$). An exact expression for C is not known, however for large values of the ratio A^2/N Shannon[1] has shown that

$$C = \frac{1}{2}\ln\frac{2}{\pi e}\frac{A^2}{N} + \epsilon_3\left(\frac{A^2}{N}\right) \tag{93}$$

where $\epsilon_3 \to 0$ as $A^2/N \to \infty$. Combining the left inequality of (92) with (93) we obtain

$$C - \ln 2 + \epsilon(A^2/N) \leqq C_B \leqq C \tag{94}$$

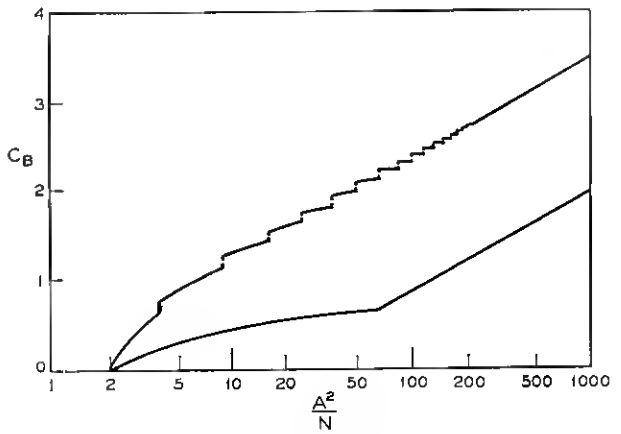

Fig. 5 (Channel B) — Upper and lower bounds on C_B vs A^2/N.

where $\epsilon \to 0$ as $A^2/N \to \infty$. Hence for large signal-to-noise ratio A^2/N, C_B differs from C by no more than a constant. Alternately $C_B/C \to 1$ as $A^2/N \to \infty$.

4.4 *Exponential Behavior of* P_{eB}

For a fixed $R < C_B$, denote by P_{eB}^* the smallest attainable value of P_{eB}, the error probability using BDD. It was shown above that $P_{eB}^* \xrightarrow{n} 0$. In this section we shall show that $P_{eB}^* = \exp[-nE_B(R) + o(n)]$ and obtain estimates of $E_B(R)$.

Given an n and R, denote by $\beta_n(R)$ the largest value of β attainable for a code of length n and with transmission rate R. With R held fixed, let $\beta(R) = \lim_{n\to\infty} \beta_n(R)$. We can estimate $\beta(R)$ in terms of R by

$$R_L(\beta(R)) \leqq R \leqq R_U(\beta(R)), \tag{95}$$

where R_L and R_U are given (17) and (18) respectively. Inequalities (95) result in upper and lower bounds on $\beta(R)$. Thus for any R there exists a code (for n sufficiently large) with minimum distance corresponding to $\beta(R)$ (i.e., $d = 2\sqrt{\beta n}$). With R fixed, this code minimizes P_{eB}. If code word $\mathbf{x}$ is transmitted and y is received, the error probability is [from (89)]

$$P_{eB}^* = \Pr[d^2(\mathbf{x},\mathbf{y}) \geqq \beta(R)n]. \tag{96}$$

This quantity depends only on the noise and not on $\mathbf{x}$. It is shown in Appendix F that

$$P_{eB}^* = \exp[-nE_B(R) + o(n)], \tag{97a}$$

where

$$E_B(R) = \frac{\hat{\beta}(R)}{2N} A^2 - \frac{1}{2} \ln \frac{A^2}{N} e\hat{\beta}(R) = \frac{\beta(R)}{2N} - \frac{1}{2} \ln \frac{e\beta(R)}{N}, \tag{97b}$$

where $\hat{\beta}(R) = \beta(R)/A^2$. The upper and lower bounds on $\beta(R)$ (95) yield corresponding bounds on $E_B(R)$. These bounds are plotted in Fig. 6 for the case $A^2/N = 10$.

V. CHANNEL C (GAUSSIAN CHANNEL WITH ENERGY CONSTRAINT)

5.1 *Lower Bound on* $M(n,\theta)$

The following bound is similar, though slightly sharper, than the

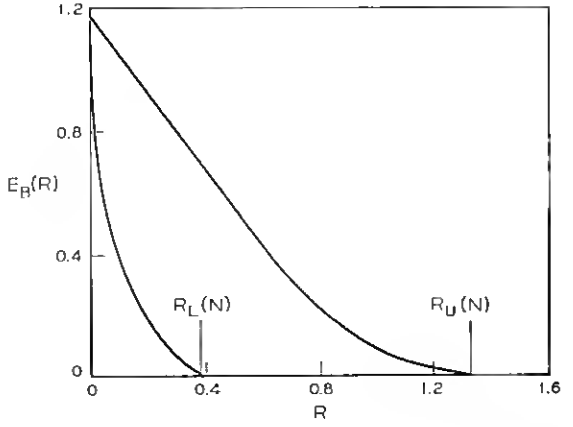

Fig. 6 (Channel B) — Upper and lower bounds on the error exponent $E_B(R)$ vs R (for $A^2/N = 10$).

lower bound on $M(n,\theta)$ obtained by Shannon.[11] The derivation used here is based on a similar argument in Blaehman.[14]

Let

$$S_n(r) = \frac{n \cdot \pi^{n/2}}{\Gamma\left(\frac{n+2}{2}\right)} \cdot r^{n-1}$$

be the surface area of a sphere in Euclidean n-spaee of radius r, and let $A_n(r,\theta)$ be the area of the n-dimensional spherical eap eut from a sphere of radius r about the origin by a right eireular eone of half angle θ with apex at the origin and axis the semi-infinite line eonnecting the origin and the point $(r,0,0,\cdots)$. It is not hard to show that

$$A_n(r,\theta) = \frac{(n-1)\pi^{(n-1)/2}}{\Gamma\left(\frac{n+1}{2}\right)} r^{n-1} \int_0^\theta \sin^{(n-2)} \varphi \, d\varphi.$$

Derivation of the Bound

For a given n and θ consider the maximum size n-dimensional code with minimum angle θ between code points. This eode has $M(n,\theta)$ eode words. About eacb code point $\mathbf{x}$, construct the spherieal eap eut from the surfaee of tbe sphere of radius $\sqrt{nP}$ about the origin by the right eireular eone witb balf angle θ and axis the semi-infinite line

joining the origin and $\mathbf{x}$. Thus the cap is the set of points $\mathbf{y}$ on the surface of the sphere such that the angle $a(\mathbf{x},\mathbf{y}) < \theta$. Now the set of all such caps (about each of the M code points) must cover the entire surface of the sphere. This is so since if $\mathbf{x}_o$ is a point on the surface of the sphere, and $\mathbf{x}_o$ is not on any cap then $a(\mathbf{x}_o, \mathbf{x}) \geqq \theta$ for all code words $\mathbf{x}$, so that $\mathbf{x}_o$ may be added to the code destroying the maximality. Since the area of each of the M caps is $A_n(\sqrt{nP},\theta)$, we have

$$M \cdot A_n(\sqrt{nP},\theta) \geqq S_n(\sqrt{nP})$$

or

$$M(n,\theta) \geqq \frac{S_n(\sqrt{nP})}{A_n(\sqrt{nP},\theta)} = \frac{n}{(n-1)} \sqrt{\pi} \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n+2}{2}\right)} \cdot \left[\int_0^\theta \sin^{(n-2)} \varphi \, d\varphi\right]^{-1}. \tag{98}$$

This result taken together with Rankin's upper bound[13] yields the following estimate of $M(n,\theta)$:

$$\frac{n}{n-1} \sqrt{\pi} \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n+2}{2}\right)} \cdot \left[\int_0^\theta \sin^{n-2} \varphi \, d\varphi\right]^{-1} \leqq M(n,\theta) \leqq \frac{\sqrt{\pi}\Gamma\left(\frac{n-1}{2}\right) \sin \psi \tan \psi}{2\Gamma\left(\frac{n}{2}\right) \int_0^\psi (\sin \varphi)^{n-2} (\cos \varphi - \cos \beta) d\varphi}, \tag{99}$$

where $\psi = \sin^{-1} \sqrt{2} \sin (\theta/2)$.

5.2 *Asymptotic Estimates of $M(n,\theta)$*

For a given n and θ, $M(n,\theta)$ is the number of points in a maximum size n-dimensional code with minimum angle between code points θ. Let the corresponding transmission rate be $R(n,\theta) = (1/n) \ln M(n,\theta)$. Now with θ held fixed, let n become large and let $R(\theta) = \lim_{n\to\infty} R(n,\theta)$.

We shall obtain upper and lower bounds on $R(\theta)$ from the behavior of (99) for large n.

Taking logarithms of both sides of inequality (99) yields

$$\frac{1}{n}\ln\frac{n}{n-1}\sqrt{\pi}+\frac{1}{n}\ln\frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n+2}{2}\right)}-\frac{1}{n}\ln\int_0^\theta \sin^{n-2}\varphi\,d\varphi$$

$$\leqq R(n,\theta) \leqq \frac{1}{n}\ln\frac{\sin\psi\tan\psi}{2}\cdot\sqrt{\pi}+\frac{1}{n}\ln\left(\frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2}\right)}\right) \tag{100}$$

$$-\frac{1}{n}\ln\int_0^\psi \sin^{n-2}\varphi(\cos\varphi-\cos\psi)\,d\psi,$$

where $\psi=\sin^{-1}\sqrt{2}\sin(\theta/2)$.

It is shown in Appendix G that

$$\lim_{n\to\infty}\frac{1}{n}\ln\int_0^\theta \sin^{n-2}\varphi\,d\varphi=\ln\sin\theta, \tag{101a}$$

and that

$$\lim_{n\to\infty}\frac{1}{n}\ln\int_0^\psi \sin^{n-2}\varphi(\cos\varphi-\cos\psi)\,d\varphi=\ln\sin\psi, \tag{101b}$$

from which we obtain (by letting $n\to\infty$),

$$-\ln\sin\theta \leqq R(\theta) \leqq -\ln\sqrt{2}\sin(\theta/2). \tag{101}$$

The bounds on $R(\theta)$ are plotted in Fig. 7.

5.3 *Bounded Discrepancy Decoding Channel Capacity*

We now assume that a code with minimum angle θ is employed and a bounded discrepancy decoder is used. We may assume, without loss of generality, that the transmitted word is $\mathbf{x}=(\sqrt{nP},0,\cdots,0)$. The received word $\mathbf{y}=(\sqrt{nP}+z_1,z_2,\cdots,z_n)$ will be correctly decoded if and only if $a(\mathbf{x},\mathbf{y})<\theta/2$. Since

$$\cos a(\mathbf{x},\mathbf{y})=\frac{\sqrt{nP}\,(\sqrt{nP}+z_1)}{\sqrt{nP}\left((\sqrt{nP}+z_1)^2+\sum_{k>1}z_k^2\right)^{\frac{1}{2}}},$$

we have

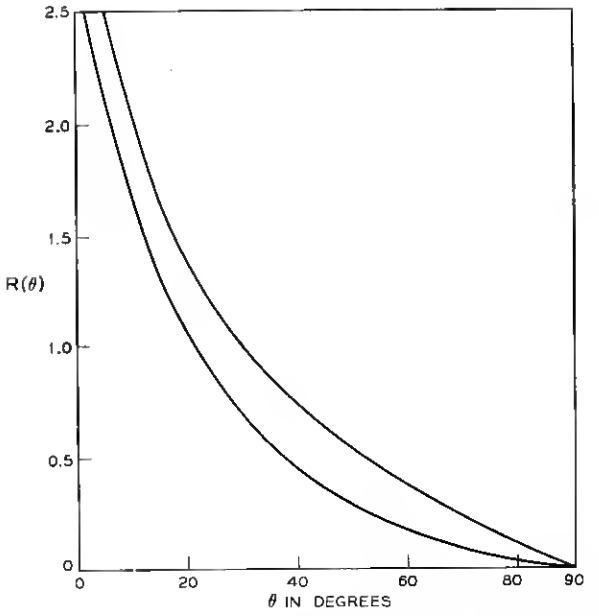

Fig. 7 (Channel C) — Upper and lower bounds on $R(\theta)$ vs θ (101).

$$\cot a = \frac{\sqrt{nP} + z_1}{\left(\sum_{k>1} z_k^2\right)^{\frac{1}{2}}} = \frac{\sqrt{P} + (z_1/\sqrt{n})}{\left(\frac{1}{n}\sum_{k>1} z_k^2\right)^{\frac{1}{2}}}.$$

Hence the probability of error is

$$P_{eB} = \Pr\left[\cot a \leqq \cot\frac{\theta}{2}\right] = \Pr\left[\frac{\sqrt{P} + z_1/\sqrt{n}}{\left(\frac{1}{n}\sum_{k>1} z_k^2\right)^{\frac{1}{2}}} \leqq \cot\frac{\theta}{2}\right]. \quad (102)$$

Now assume that for each n we use a code with minimum angle θ. We shall show that $P_{eB} \xrightarrow{n} 0$ or 1 according as $\cot(\theta/2) < \sqrt{P/N}$ or $\cot(\theta/2) > \sqrt{P/N}$: Recalling that z_k $(k = 1, \cdots, n)$ are independent normally distributed random variables with mean zero and variance N we obtain

$$\sqrt{P} + z_1/\sqrt{n} \xrightarrow{\text{Prob.}} \sqrt{P},$$

and

$$\frac{1}{n}\sum_{k>1} z^2 \xrightarrow{\text{Prob.}} N.$$

Thus the ratio

$$\frac{\sqrt{P} + z_1/\sqrt{n}}{\left(\frac{1}{n}\sum_{k>1} z_k^2\right)^{\frac{1}{2}}} \xrightarrow{\text{Prob.}} \sqrt{\frac{P}{N}}. \tag{103}$$

If cot $(\theta/2) < \sqrt{P}/N$, then $\sqrt{P}/N - \text{eot } (\theta/2) = \epsilon > 0$ so that from (102) and (103)

$$P_B(e) = \Pr\left[\sqrt{\frac{P}{N}} - \frac{\sqrt{P} + z_1/\sqrt{n}}{\left(\frac{1}{n}\sum_{k>1} z_k^2\right)^{\frac{1}{2}}} > \epsilon\right] \xrightarrow{n} 0.$$

Similarly if eot $(\theta/2) > \sqrt{P}/N$, $P_B(e) \xrightarrow{n} 1$.

Henee we can obtain vanishingly small error probability by choosing $\theta > 2$ are cot $\sqrt{P}/N$ or $\theta > 2$ arc sin $(1 + P/N)^{-\frac{1}{2}}$. The *bounded discrepancy decoding channel capacity* C_B is defined as the supremum of rates for whieh it is possible to aehieve $P_{eB} \xrightarrow{n} 0$, or equivalently the largest rate for whieh $\theta > 2$ are sin $[1 + (P/N)]^{-\frac{1}{2}}$; i.e., $C_B = R\{2 \text{ are sin } [1 + (P/N)]^{-\frac{1}{2}}\}$. Since the ehannel eapacity is $C = \frac{1}{2} \ln [1 + (P/N)]$, we may write $[1 + (P/N)]^{-\frac{1}{2}} = e^{-C}$, hence $C_B = R(2 \text{ arc sin } e^{-C})$. We estimate C_B from inequality (101):

$$-\ln \sin (2 \sin^{-1} e^{-C}) \leqq C_B \leqq -\ln \sqrt{2} e^{-C}. \tag{104}$$

Using sin $2A = 2 \sin A$ eos A, the left member of (104) becomes $-\ln 2e^{-C}$ eos $\sin^{-1} e^{-C}$. Sinee cos $\sin^{-1} e^{-C} = (1 - e^{-2C})^{\frac{1}{2}}$, incquality (104) becomes

$$C - \ln 2 - \tfrac{1}{2} \ln (1 - e^{-2C}) \leqq C_B \leqq C - \tfrac{1}{2} \ln 2. \tag{105}$$

Inequality (105) is plotted in Figs. 8(a) and 8(b). We scc that $C_B = 0$ for $C \leqq \frac{1}{2} \ln 2$ or $P/N \leqq 1$, and $C_B/C \to 1$ as $P/N \to \infty$.

5.4 *Exponential Behavior of* P_{eB}

In this seetion we show that for a fixed rate $R < C_B$, the smallest attainable probability of error $P_{eB}^* = \exp [-nE_B(R) + o(n)]$, and obtain estimates of $E_B(R)$. Given an n and R, denote by $\theta_n(R)$ the largest minimum angle attainable for an n-dimensional code with transmission rate R. With R held fixed, let $\theta(R) = \lim_{n\to\infty} \theta_n(R)$. From inequality (101)

$$-\ln \sin \theta(R) \leqq R \leqq -\ln \sqrt{2} \sin [\theta(R)/2],$$

from whieh

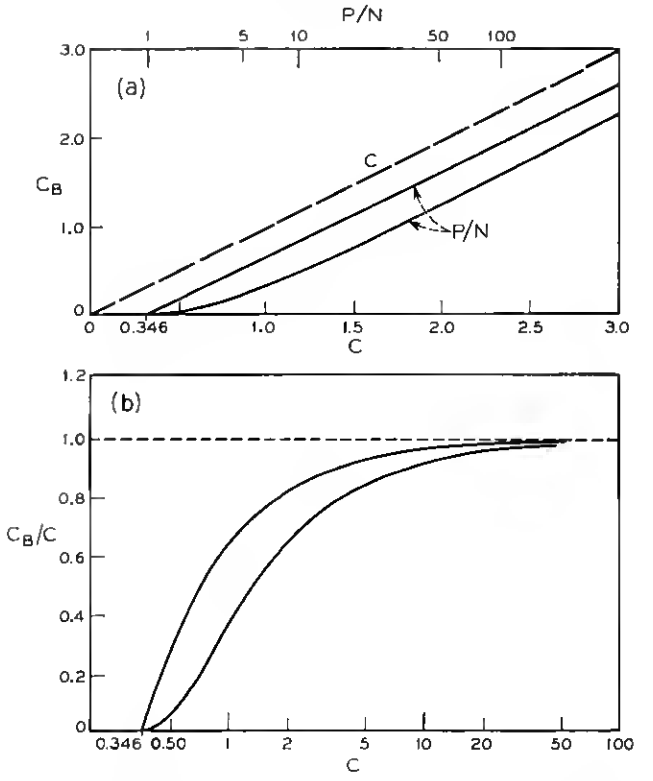

Fig. 8(a) (Channel C) — Upper and lower bounds on C_B vs C and P/N (solid lines).
Fig. 8(b) (Channel C) — Upper and lower bounds on C_B/C vs C.

$$\tfrac{1}{2} \sin^{-1} e^{-R} \leqq \theta(R)/2 \leqq \sin^{-1} (e^{-R}/\sqrt{2}). \tag{106}$$

Thus for every R there exists a code (for n sufficiently large) with minimum angle $\theta(R)$, where $\theta(R)$ is estimated by (106). For such a code P_{eB} is minimized. If code word $\mathbf{x}$ is transmitted and $\mathbf{y}$ received, the error probability is

$$P_{eB}{}^{*} = \Pr\,[a(\mathbf{x},\mathbf{y}) > \theta(R)/2]. \tag{107}$$

This quantity depends only on the noise (and not on $\mathbf{x}$). Shannon [Ref. 11, equation (4)] has obtained an expression for the asymptotic behavior of (107), which shows that

$$P_{eB}{}^{*} = \exp\,[-nE_B(R) + o(n)] \tag{108}$$

where

$$E_B(R) = \frac{P}{2N} - \frac{1}{2}\sqrt{\frac{P}{N}}\, G \cos\frac{\theta}{2} - \ln G \sin\frac{\theta}{2}$$

$$\theta = \theta(R) \tag{109}$$

$$G = \frac{1}{2}\left(\sqrt{\frac{P}{N}}\cos\frac{\theta}{2} + \sqrt{\frac{P}{N}\cos^2\frac{\theta}{2} + 4}\right).$$

The bounds on $\theta(R)$ in (106) yield corresponding bounds on $E_B(R)$. These bounds are plotted in Fig. 9.

VI. CHANNEL D (CONTINUOUS CHANNEL WITH AMPLITUDE CONSTRAINT):

As in the previous sections we begin by obtaining bounds on $M(n,\rho)$, the maximum number of points in an n-dimensional code with discrepancy ρ.

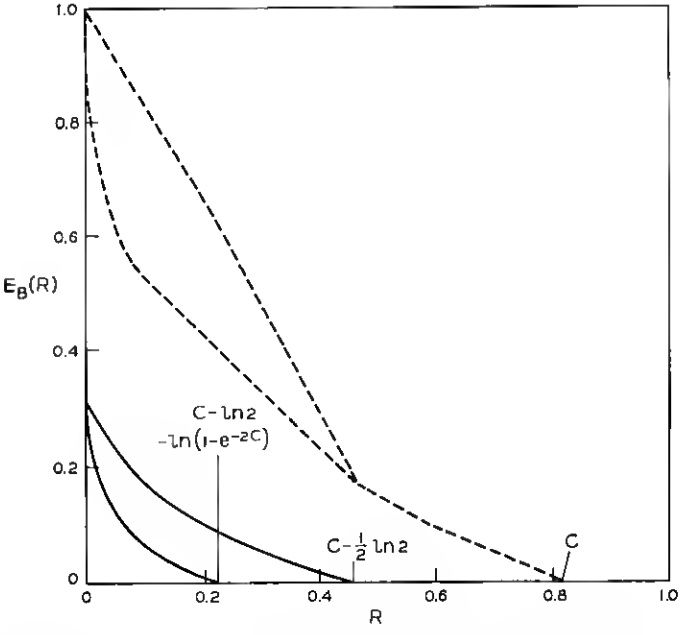

Fig. 9 (Channel C) — Upper and lower bounds on the exponent $E_B(R)$ vs R for $P/N = 4$. Upper and lower bounds on $E(R)$ are in dotted lines.

6.1 *Upper Bound on $R(\beta)$*

We have defined $S_n(\mathbf{x},\rho)$ as the region consisting of those vectors $\boldsymbol{\alpha} \in \mathcal{C}_n$ for which $d_o(\mathbf{x},\boldsymbol{\alpha}) < \rho$. Applying the Euclidean measure to $\mathcal{C}_n$ in the obvious way, we set $V_n(\mathbf{x},\rho)$ equal to the volume of $S_n(\mathbf{x},\rho)$. Now consider a maximum size n-dimensional code with discrepancy ρ consisting of $M = M(n,\rho)$ points $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_M$. Since the regions $S_n(\mathbf{x}_i, \rho)$ about each of the M code points $\mathbf{x}_i$ are disjoint,

$$\sum_{i=1}^{M} V_n(\mathbf{x}_i, \rho) \leqq \text{volume of } \mathcal{C}_n = (2A)^n. \tag{110}$$

Since $V_n(\mathbf{x}_i, \rho)$ is independent of $\mathbf{x}_i$ (due to the homogeneity of $\mathcal{C}_n$ brought about by wrapping the interval onto the circumference of a circle) we set $V_n(\mathbf{x}_i, \rho) = V_n(\rho)$, and (110) yields

$$M(n,\rho) \leqq (2A)^n / V_n(\rho), \tag{111}$$

thus

$$R(n,\rho) = \frac{1}{n} \ln M(n,\rho) \leqq \frac{1}{n} \ln \frac{(2A)^n}{V_n(\rho)}. \tag{112}$$

If we set $\rho = \beta n$ and let $n \to \infty$ while β is held fixed we obtain

$$R(\beta) \leqq \lim \frac{1}{n} \ln \frac{(2A)^n}{V_n(\rho n)} = R_U(\beta). \tag{113}$$

It is shown in Appendix C that $R_U(\beta) = C_o(\beta)$ which establishes our upper bound.

6.2 *Lower Bound on $R(\beta)$*

Again let us consider a maximum size code with discrepancy ρ and $M = M(n,\rho)$ code words. About each of the code words $\mathbf{x}_i$ ($i = 1, 2, \cdots, M$) consider the region $S_n(\mathbf{x}_i, 2\eta\rho)$ where

$$\eta = \sup_{-A \leqq u_1, u_2 \leqq +A} \frac{r(u_1 \dot{+} u_2)}{r(u_1) + r(u_2)}. \tag{114}$$

We claim that the union of these regions $\bigcup_{i=1}^{M} S_n(\mathbf{x}_i, 2\eta\rho)$ contains $\mathcal{C}_n$. First let us observe that by definition of η,

$$r(u_1 \dot{+} u_2) \leqq \eta[r(u_1) + r(u_2)],$$

so that for $\mathbf{x},\mathbf{y},\mathbf{z} \in \mathcal{C}_n$,

$$d_o(\mathbf{x},\mathbf{y}) = \sum_{k=1}^{n} r(x_k \dot{-} y_k) \leqq \eta\Big[\sum_k r(x_k \dot{-} z_k) + \sum_k r(z_k \dot{-} y_k)\Big]$$
$$= \eta d_o(\mathbf{x},\mathbf{z}) + \eta d_o(\mathbf{z},\mathbf{y}). \tag{115}$$

Now suppose there existed a vector $\mathbf{x}_o \in \mathcal{C}_n$ such that $\mathbf{x}_o \notin \bigcup_{i=1}^{M} S_n(\mathbf{x}_i, 2\eta\rho)$. Then

$$d_o(\mathbf{x}_o, \mathbf{x}_i) \geqq 2\eta\rho \tag{116}$$

for each code word $\mathbf{x}_i$ $(i = 1, 2, \cdots, M)$. Let $\boldsymbol{\alpha} \in S_n(\mathbf{x}_i, \rho)$ for some code word $\mathbf{x}_i$ so that $d_o(\boldsymbol{\alpha},\mathbf{x}_i) < \rho$, hence from (115) and (116) we have

$$d_o(\mathbf{x}_o, \boldsymbol{\alpha}) \geqq (1/\eta) d_o(\mathbf{x}_o, \mathbf{x}_i) - d_o(\mathbf{x}_i, \boldsymbol{\alpha}) > (1/\eta)(2\eta\rho) - \rho = \rho. \tag{117}$$

We conclude from (117) that $\boldsymbol{\alpha} \notin S_n(\mathbf{x}_o, \rho)$, so that $S_n(\mathbf{x}_o, \rho) \cap S_n(\mathbf{x}_i, \rho)$ is empty for all code words $\mathbf{x}_i$, and $\mathbf{x}_o$ may be added to the code destroying the maximality. Thus we conclude that

$$\mathcal{C}_n \subseteq \bigcup_{i=1}^{M} S_n(\mathbf{x}_i, 2\eta\rho). \tag{118}$$

As in the previous section, let $V_n(2\eta\rho)$ be the volume of $S_n(\mathbf{x}_i, 2\eta\rho)$. From (118) we have

$$\text{volume of } \mathcal{C}_n = (2A)^n \leqq M \cdot V_n(2\eta\rho),$$

or

$$M(n,\rho) \geqq \frac{(2A)^n}{V_n(2\eta\rho)}. \tag{119}$$

Again as in the previous section,

$$R(\beta) \geqq \lim \frac{1}{n} \ln \frac{(2A)^n}{V_n(2\eta\beta n)} = R_L(\beta). \tag{120}$$

It is shown in Appendix C that $R_L(\beta) = C_o(2\eta\beta)$, establishing our lower bound.

6.3 *Bounded Discrepancy Decoding Channel Capacity*

Suppose that for every n, an n-dimensional code is available with

discrepancy $\rho = \beta n$ (β fixed). Using bounded discrepancy decoding we have error probability

$$P_{eB} = \Pr [d_o(\mathbf{x},\mathbf{y}) \geqq \rho] = \Pr [d_o(\mathbf{x},\mathbf{y}) \geqq \beta n], \tag{121}$$

where $\mathbf{x}$ is the transmitted word and $\mathbf{y}$ is the received vector. Since $d_o(\mathbf{x},\mathbf{y}) = \sum_{k=1}^{n} r(z_k)$, where the z_k are the statistically independent noise components, we have

$$P_{eB} = \Pr\left[\sum_{k=1}^{n} r(z_k)/n > \beta\right]. \tag{122}$$

By the weak law of large numbers, $\sum_{k=1}^{n} r(z_k)/n$ tends in probability to $N(= E(r(z_k)))$. Thus $\lim_{n\to\infty} P_{eB} = 0$ or 1 according as $\beta < N$ or $\beta > N$.

We have defined the *bounded discrepancy decoding channel capacity* denoted by C_B as the supremum of the rates for which it is possible (asymptotically in n) to obtain vanishingly small error probability using bounded discrepancy decoding. From the foregoing we see that $C_B = R(N)$. Making use of the bounds on $R(\beta)$ established above we have

$$C_o(2\eta N) \leqq C_B \leqq C_o(N) = C, \tag{123}$$

where C is the channel capacity (the supremum of those rates for which it is possible (asymptotically in n) to obtain vanishing small error probability using (optimum) minimum discrepancy decoding). The error exponent $E_B(R)$ could be estimated exactly as for channel B in Section IV.

Thus it is an open question whether C_B is *strictly* less than the channel capacity. In the special case of the quadratic discrepancy where $r(u) = u^2$, i.e., the case where $p(u) = K_o \exp(-\lambda u^2)$, it is possible to show that $C_B < C$. This is done in the following section.

6.4 *The Quadratic Discrepancy*

We now consider the case of the quadratic discrepancy where $r(u) = u^2$, which corresponds to a noise probability density function $p(u) = K_o \exp(-\lambda u^2)$, and a discrepancy function

$$d_o(\mathbf{x},\mathbf{y}) = \sum_{k=1}^{n} (x_k \dot{-} y_k)^2.$$

Note that the subtraction $x_k \dot{-} y_k$ is performed modulo $2A$ with the

difference reduced into the interval $[-A,A]$, but the squaring and summing operations are ordinary arithmetic.

Let us first observe that

$$\frac{r(u_1 \dot{+} u_2)}{r(u_1) + r(u_2)} \leqq \frac{(u_1 + u_2)^2}{u_1^2 + u_2^2} = 1 + \frac{u_1 u_2}{\left(\frac{u_1^2 + u_2^2}{2}\right)}.$$

Since for any two numbers u_1^2 and u_2^2, the algebraic mean $(u_1^2 + u_2^2)/2$ is not less than the geometric mean $u_1 u_2$,

$$\frac{r(u_1 \dot{+} u_2)}{r(u_1) + r(u_2)} \leqq 1 + 1 = 2.$$

Thus, since this value is achieved when $u_1 = u_2 \leqq A/2$, $\eta = 2$. The lower bound on $R(\beta)$ (34) is therefore

$$R(\beta) \geqq C_o(4\beta). \tag{124}$$

6.4.1 *Upper Bound on $R(\beta)$*

Now we establish a new upper bound on $R(\beta)$ for this special case. First we need the following

Lemma: Let $\mathbf{x}_\nu = (x_{\nu 1}, x_{\nu 2}, \cdots, x_{\nu n})$, $\nu = 1, 2, \cdots, m$, *be any m points selected from a code with discrepancy* $\rho = \beta n$. *Let* $\mathbf{y}$ *be any n-vector and let* $d_\nu = d_o(\mathbf{x}_\nu, \mathbf{y})$, $\nu = 1, 2, \cdots, m$. *Then*

$$\sum_{\nu=1}^{m} d_\nu \geqq 2(m-1)\rho.$$

Proof: First we show that for $1 \leqq \mu < \nu \leqq m$ that

$$d_o(\mathbf{x}_\nu, \mathbf{x}_\mu) \geqq 4\rho. \tag{125}$$

To show this consider the vector $\mathbf{z} \in \mathcal{C}_n$:

$$\mathbf{z} = \left(\frac{x_{\nu 1} \dot{+} x_{\mu 1}}{2}, \frac{x_{\nu 2} \dot{+} x_{\mu 2}}{2}, \cdots, \frac{x_{\nu n} \dot{+} x_{\mu n}}{2}\right).$$

The addition $x_{\nu k} \dot{+} x_{\mu k}$ is, as always, modulo $2A$. Clearly

$$d_o(\mathbf{x}_\nu, \mathbf{z}) = d_o(\mathbf{x}_\mu, \mathbf{z}) = \sum_{k=1}^{n} \frac{(x_{\nu k} \dot{-} x_{\mu k})^2}{4} = \frac{d_o(\mathbf{x}_\nu, \mathbf{x}_\mu)}{4}. \tag{126}$$

Since the regions $S_n(\mathbf{x}_\nu, \rho)$ and $S_n(\mathbf{x}_\mu, \rho)$ are disjoint, $d_o(\mathbf{x}_\nu, \mathbf{z})$, $d_o(\mathbf{x}_\mu, \mathbf{z}) \geqq \rho$. Thus (126) yields $d_o(\mathbf{x}_\nu, \mathbf{x}_\mu) \geqq 4\rho$. We now continue with the proof of the lemma.

Without loss of generality take $\mathbf{y} = 0$ so that $d_\nu = \sum_{k=1}^{n} x_{\nu k}^2$. Since $d_o(\mathbf{x}_\nu, \mathbf{x}_\mu) \geqq 4\rho$ $(\mu < \nu)$,

$$\begin{aligned}\binom{m}{2} 4\rho &\leqq \sum_{1 \leqq \mu < \nu \leqq m} d_o(\mathbf{x}_\mu, \mathbf{x}_\nu) = \sum_{k=1} \sum_{\mu<\nu} (x_{\mu k} - x_{\nu k})^2 \\ &\leqq \sum_k \sum_{\mu<\nu} (x_{\mu k} - x_{\nu k})^2 \qquad (127) \\ &= m \sum_\nu \sum_k x_{\nu k}^2 - \sum_k \Big(\sum_\nu x_{\nu k}\Big)^2 \leqq m \sum_\nu d_\nu .\end{aligned}$$

The lemma follows on dividing through by m. We now obtain the upper bound on $R(\beta)$.

Consider again a maximum size n-dimensional code with discrepancy ρ and with $M = M(n,\rho)$ code words $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_M$. Consider the regions $S_n(\mathbf{x}_\nu, 2\rho)$ about each of the code words $\mathbf{x}_\nu$ $(\nu = 1, 2, \cdots, M)$. These regions are not necessarily disjoint. At each point $\mathbf{y}$ in $S_n(\mathbf{x}_\nu, 2\rho)$ define a density $\sigma(d)$:

$$\sigma(d) = 2\rho - d, \qquad (128)$$

where d is the discrepancy $d_o(\mathbf{x}_\nu, \mathbf{y})$. The mass of each region is

$$\mu = \int_{d<2\rho} \sigma(d)\, dV. \qquad (129)$$

If a vector $\mathbf{y} \in \mathcal{C}_n$ belongs simultaneously to the regions about the m code points $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_m$, we assign to $\mathbf{y}$ a density equal to the sum of the densities contributed by each region; i.e.,

$$\sigma_{\mathbf{y}} = \sum_{\nu=1}^{m} \sigma(d_\nu) = 2m\rho - \sum_{\nu=1}^{m} d_\nu , \qquad (130)$$

where $d_\nu = d(\mathbf{x}_\nu, \mathbf{y})$. Thus we have

$$\text{mass of } \mathcal{C}_n = \int_{\mathcal{C}_n} \sigma_{\mathbf{y}} dV = M(n,\rho) \cdot \mu. \qquad (131)$$

We will bound $M(n,\rho)$ by finding an upper bound on the mass of $\mathcal{C}_n$.

By applying the above lemma to (130) we obtain

$$\sigma_{\mathbf{y}} \leqq 2m\rho - 2(m-1)\rho = 2\rho. \qquad (132)$$

Thus

$$\text{mass of } \mathcal{C}_n \leqq (2\rho)\ (\text{volume of } \mathcal{C}_n) = 2\rho(2A)^n. \qquad (133)$$

Applying (133) to (131) yields

$$M(n,\rho) \leqq \frac{2\rho(2A)^n}{\mu}. \tag{134}$$

Now,

$$\mu = \int_{d<2\rho} (2\rho - d)\,dV \geqq \int_{d<2\rho-1} dV = V_n(2\rho - 1) \tag{135}$$

where $V_n(2\rho - 1)$ is the volume of the region $S_n(\mathbf{x},2\rho - 1)$ (which is independent of $\mathbf{x}$). Applying (135) to (134) yields

$$M(n,\beta n) \leqq \frac{2\beta n(2A)^n}{V_n(2\beta n - 1)} \tag{136}$$

where $\rho = \beta n$. Applying the result of Appendix C to (136) yields

$$R(\beta) = \lim_{n\to\infty} (1/n) \ln M(n,\beta n) \leqq C_o(2\beta). \tag{137}$$

This is our upper bound.

6.4.2 *Refinements of Bounds for Large β/A^2*

The upper and lower bounds on $R(\beta)$ obtained above are plotted vs. β/A^2 in Fig. 10. It can be seen that these bounds diverge for large

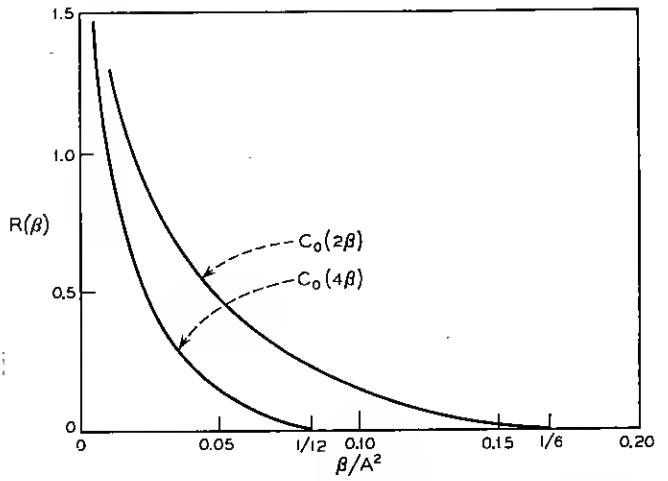

FIG. 10 (Channel D) — Upper and lower bounds on $R(\beta)$ vs β/A^2 for quadratic discrepancy.

values of β/A^2. We will now obtain new upper and lower bounds on $R(\beta)$ which in fact converge at $\beta/A^2 = \frac{1}{8}$.

6.4.2.1 *Upper Bound*

A new upper bound on $R(\beta)$ will be obtained which will tell us that $R(\beta) = 0, \beta/A^2 > \frac{1}{8}$. First we need the following:

Lemma: Let $a_1, a_2, \cdots, a_m$ *be a set of real numbers such that* $-A \leqq a_j \leqq +A, j = 1, 2, \cdots, m$. *Then*

$$\sum_{1 \leqq i < j \leqq m} (a_i \dot{-} a_j)^2 \leqq A^2 m^2/4.$$

Note that, as usual, the difference $(a_i \dot{-} a_j)$ is performed modulo $2A$ with the result reduced into the interval $[-A,+A]$, and the squaring and summing operations are ordinary arithmetic.

Proof: Let us wrap the interval $[-A,+A]$ onto the circumference of a circle of radius A/π (so that the circumference is $2A$). Denote by

$$d_c(a_i, a_j) = |(a_i \dot{-} a_j)|,$$

the circumferential distance between a_i and a_j, and by $d_E(a_i, a_j)$ the Euclidean distance between a_i and a_j (see Fig. 11). It is easy to see that

$$d_E(a_i, a_j) = 2\frac{A}{\pi} \sin \frac{1}{2} \frac{d_c(a_i, a_j)}{(A/\pi)}. \tag{138}$$

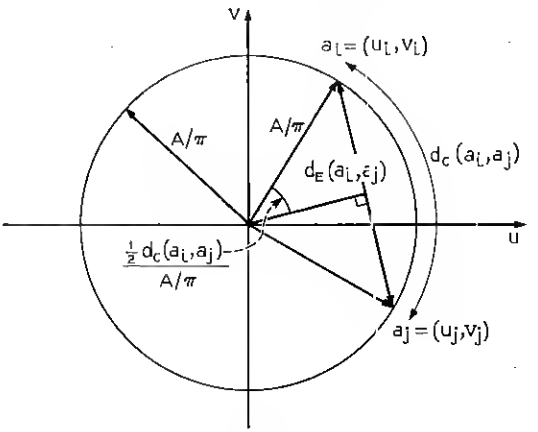

Fig. 11 — Diagram illustrating proof of lemma.

Since, for $0 \leqq x \leqq \pi/2$, $\sin x \geqq (2/\pi)x$, (138) yields

$$d_E(a_i, a_j) \geqq (2/\pi)\, d_c(a_i, a_j). \tag{139}$$

Now taking the origin to be the center of the circle, we may assign Cartesian coordinates (u_j, v_j) to the point a_j, where

$$u_j^2 + v_j^2 = A^2/\pi^2. \tag{140}$$

Thus from (139) we have

$$\sum_{i<j} (a_i \dot{-} a_j)^2 = \sum_{i<j} d_c^2(a_j, a_j) \leqq \frac{\pi^2}{4} \sum_{i<j} d_E^2(a_i, a_j). \tag{141}$$

Since $d_E^2(a_i, a_j) = (u_i - u_j)^2 + (v_i - v_j)^2$, we have

$$\begin{aligned} \sum_{i<j} (a_i \dot{-} a_j)^2 &\leqq \frac{\pi^2}{4} \sum_{i<j} \{(u_i - u_j)^2 + (v_i - v_j)^2\} \\ &= \frac{\pi^2}{4} \left\{ \sum_{j=1}^{m} m(u_j^2 + v_j^2) - \left(\sum_j u_j\right)^2 - \left(\sum_j v_j\right)^2 \right\} \\ &\leqq \frac{\pi^2}{4} \left\{ \sum_{j=1}^{m} m\left(\frac{A^2}{\pi^2}\right) \right\} \\ &= \frac{A^2 m^2}{4}. \end{aligned} \tag{142}$$

Hence the lemma.

Derivation of the Bound

Suppose we have a maximum size code with discrepancy ρ and $M = M(n,\rho)$ code words $\mathbf{x}_\nu = (x_{\nu 1}, x_{\nu 2}, \cdots, x_{\nu n})$, $\nu = 1, 2, \cdots, M$. We have shown [inequality (125)] that $d(x_\mu, x_\nu) \geqq 4\rho$ $(\mu \neq \nu)$. Thus, making use of the above lemma, we have

$$\begin{aligned} \binom{M}{2} 4\rho &\leqq \sum_{1 \leqq \mu < \nu \leqq M} d_c(\mathbf{x}_\nu, \mathbf{x}_\mu) = \sum_{k=1}^{n} \sum_{\mu<\nu} (x_{\mu k} \dot{-} x_{\nu k})^2 \\ &\leqq \sum_{k=1}^{n} \frac{A^2 M^2}{4} = \frac{A^2 M^2 n}{4}, \end{aligned}$$

so that for $\beta = \rho/n > A^2/8$,

$$M = M(n,\rho) \leqq \frac{8\rho}{8\rho - A^2 n} = \frac{\beta}{\beta - \frac{A^2}{8}}. \tag{143}$$

Hence,

$$R(n,\rho) = \frac{1}{n} \ln M(n,\rho) \leqq \frac{1}{n} \ln \frac{\beta}{\beta - \frac{A^2}{8}}. \tag{144}$$

Letting $n \to \infty$ with β held fixed we obtain for $\beta/A^2 > \frac{1}{8}$,

$$R(\beta) = \lim_{n \to \infty} R(n,\beta n) = 0. \tag{145}$$

In a manner similar to that used in Section IV we can use (143) to obtain the following bound on $R(\beta)$ valid for $\beta/A^2 < \frac{1}{8}$:

$$R(\beta) \leqq 9 \ (\ln 3) \ [1 - (8\beta/A^2)]. \tag{146}$$

As is evident from Fig. 12, inequality (146) does not yield much improvement in our upper bound, hence the derivation is omitted.

6.4.2.2 *Lower Bound*

A new lower bound on $R(\beta)$ will now be obtained. This bound is always sharper than the previously obtained bound $R(\beta) \geqq C_o(4N)$, however the best improvement is for large β/A^2.

Suppose that we require that x_k be one of the following m points on the interval $[-A,+A]$, where m is an even integer:

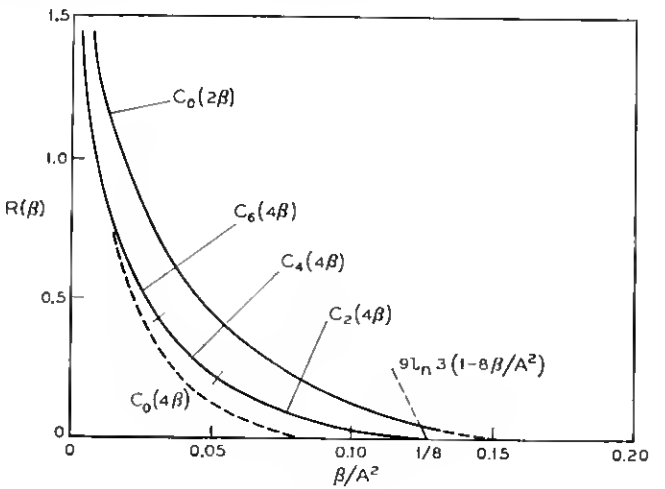

Fig. 12 (Channel D) — Refined upper and lower bounds on $R(\beta)$ vs β/A^2 for quadratic discrepancy.

$$0, \pm\frac{2A}{m}, \pm 2\left(\frac{2A}{m}\right), \pm 3\left(\frac{2A}{m}\right), \cdots, \pm\left(\frac{m-2}{2}\right)\left(\frac{2A}{m}\right), A. \quad (147)$$

Such a code certainly satisfies the requirements set forth in Section II. In the exactly the same manner that the previously derived lower bound $R(\beta) \geqq C_o(4\beta)$ was obtained, we can show that

$$R(\beta) \geqq C_m(4\beta)$$

where

$$C_m(\xi) = \ln AK_m(\xi) - \xi\lambda_m(\xi), \quad (148)$$

where $\lambda_m(\xi)$ is defined by

$$\sum_k u_k^2 e^{-\lambda u_k^2} = \xi \sum_k e^{-\lambda u_k^2}, \quad (149a)$$

and $K_m(\xi)$ is

$$K_m(\xi) = [\sum_k e^{-\lambda(\xi) u_k^2}]^{-1}, \quad (149b)$$

where the u_k are the m points of (147).

Since no value of m yields a uniformly strongest bound we write

$$R(\beta) \geqq \max_{m \text{ even}} C_m(4\beta). \quad (150)$$

This new bound is plotted in Fig. 12. Let us observe that the lower bound $R(\beta) \geqq C_2(4\beta)$, and the upper bound $R(\beta) \leqq 9 \ln 3[1 - (8\beta/A^2)]$ agree when $\beta/A^2 = \frac{1}{8}$. Thus $C_B = 0$ for $\beta/A^2 \geqq \frac{1}{8}$.

6.4.3 *Estimation of C_B*

We now obtain an estimate of C_B for the case of a quadratic discrepancy function. As discussed above $C_B = R(N)$. The bounds on $R(\beta)$ of (137), (146), (150) yield

$$\max_{m \text{ even}} C_m(4N) \leqq C_B \leqq \min \begin{cases} C_o(2N), \\ 9 \ln 3\left(1 - \dfrac{8N}{A^2}\right). \end{cases} \quad (151)$$

Since the channel capacity $C = C_o(N) > C_o(2N)$, the first upper bound of (151) implies that C_B is strictly less than the channel capacity C. For large values of the "signal-to-noise" ratio A^2/N, the left side of (151) may be approximated by $C_o(4N)$. We can make use of the asymptotic form of $C_o(\xi)$ obtained in Appendix D:

$$C_o(\xi) = \tfrac{1}{2} \ln (2A^2/\pi e\xi) + \epsilon(\xi), \quad (152)$$

where $\epsilon(\xi) \to 0$ as $\xi \to 0$. Applying (152) to (151), we obtain

$$\tfrac{1}{2} \ln \frac{A^2}{2\pi eN} + \epsilon_1\left(\frac{A^2}{N}\right) \leqq C_B \leqq \tfrac{1}{2} \ln \frac{A^2}{\pi eN} + \epsilon_2\left(\frac{A^2}{N}\right), \quad (153)$$

where ϵ_1, $\epsilon_2 \to 0$ as $A^2/N \to \infty$. Furtber since the channel capacity C is (for large A^2/N)

$$C = C_o(N) = \tfrac{1}{2} \ln \frac{2}{\pi e} \frac{A^2}{N} + \epsilon_3\left(\frac{A^2}{N}\right), \quad (154)$$

where $\epsilon_3 \to 0$ as $A^2/N \to \infty$, (153) may be rewritten as

$$C - \ln 2 + \epsilon_5(A^2/N) \leqq C_B \leqq C - \tfrac{1}{2} \ln 2 + \epsilon_6(A^2/N), \quad (155)$$

where ϵ_5, $\epsilon_6 \to 0$ as $A^2/N \to \infty$. Thus for large values of A^2/N (and hence C), the bounded discrepancy channel capacity C_B differs by no more than a constant (ln 2) from the channel capacity C. Tbus the ratio $C_B/C \to 1$ as $A^2/N \to \infty$.

Let us remark at this point that the cbannel capacity of the Gaussian channel with amplitude constraint has been shown by Shannon[1] to be approximately $C_o(N)$ (for large A^2/N), which is the same as the capacity of the present channel. This fact lends plausibility to the claim that the present channel is an approximation to the Gaussian amplitude constrained channel for large values of A^2/N.

APPENDIX A

In this appendix we show that for any function $r(u)$ for which $r(u) \to 0$ as $u \to 0$, and for any ξ satisfying

$$0 < \xi \leqq \frac{1}{A} \int_0^A r(u)\, du, \quad (156)$$

there exists a unique $\lambda(\xi)$ whieh satisfies

$$\int_0^A r(u) e^{-\lambda(\xi) r(u)} du = \xi \int_0^A e^{-\lambda(\xi) r(u)} du. \quad (157)$$

For channel B we are interested in the case $r(u) = u^2$, however for channel D we need this proposition for arbitrary $r(u)$. If we define thc function $\xi(\lambda)$ by

$$\xi(\lambda) = \frac{\int_0^A r(u) e^{-\lambda r(u)} du}{\int_0^A e^{-\lambda r(u)} du}, \qquad 0 \leqq \lambda < \infty, \quad (158)$$

it will suffice to show that

(a) $\xi(\lambda)$ is strictly monotone decreasing,

(b) $\xi(0) = \frac{1}{A}\int_0^A r(u)\,du,$

(c) $\lim_{\lambda\to\infty} \xi(\lambda) = 0.$

If (a), (b) and (c) are true, $\xi(\lambda)$ is a one-to-one mapping of the half line $[0, \infty)$ onto the interval

$$\left(0, \frac{1}{A}\int_0^A r(u)\,du\right].$$

(a) To show that $\xi(\lambda)$ is monotone decreasing, consider

$$\frac{d\xi(\lambda)}{d\lambda} = \frac{-\left(\int_0^A e^{-\lambda r}du\right)\left(\int_0^A r^2 e^{-\lambda r}du\right) + \left(\int_0^A re^{-\lambda r}du\right)^2}{\left(\int_0^A e^{-\lambda r}du\right)^2}, \quad (159)$$

by the Schwarz inequality,

$$\left(\int_0^A re^{-\lambda r}du\right)^2 < \left(\int_0^A r^2e^{-\lambda r}du\right)\left(\int_0^A e^{-\lambda r}du\right), \quad (160)$$

(the strict inequality holding). Thus $d\xi(\lambda)/d\lambda < 0$ and (a) is established.

$$(b)\quad \xi(0) = \int_0^A r(u)\,du \Big/ \int_0^A du = \frac{1}{A}\int_0^A r(u)\,du.$$

(c) (due to H. O. Pollak†) since $\xi(\lambda)$ is monotone decreasing and positive for $\lambda < \infty$, we know that $\lim_{\lambda\to\infty} \xi(\lambda) = \beta \geqq 0$. If $\beta = 0$ (c) is established. Thus we assume the contrary, i.e., $\beta > 0$. Since $\xi(\lambda)$ is monotone decreasing we have $\xi(\lambda) \geqq \beta$, all $\lambda < \infty$. Thus for any Λ,

$$\int_0^\Lambda \xi(\lambda)\,d\lambda \geqq \beta\Lambda. \quad (161)$$

Now let us observe that $\xi(\lambda)$ may be written

$$\xi(\lambda) = -\frac{d}{d\lambda}\left(\ln \int_0^A e^{-\lambda r(u)}du\right). \quad (162)$$

† An alternate proof was given to the author by L. A. Shepp.

Substituting (162) into (161) we obtain

$$\int_0^\Lambda \xi(\lambda)\,d\lambda = -\ln \int_0^\Lambda e^{-\Lambda r(u)}du + \ln A \geqq \beta\Lambda. \tag{163}$$

Or,

$$\frac{1}{A}\int_0^A e^{-\Lambda r(u)}du \leqq e^{-\beta\Lambda}. \tag{164}$$

Dividing through by $e^{-\beta\Lambda}$ we have

$$\frac{1}{A}\int_0^A e^{+\Lambda(\beta - r(u))}du \leqq 1. \tag{165}$$

Now since $r(u) \to 0$ as $u \to 0$, choose δ sufficiently small so that $r(u) < \beta/2$ whenever $0 \leqq u \leqq \delta$. Equation (165) now becomes

$$\begin{aligned} 1 &\geqq \frac{1}{A}\int_0^A e^{+\Lambda(\beta - r)}du \\ &\geqq \frac{1}{A}\int_0^\delta e^{+\Lambda(\beta - r(u))}du \\ &\geqq \frac{1}{A}\,e^{\Lambda\beta/2}\int_0^\delta du = \frac{\delta}{A}\,e^{\Lambda\beta/2}. \end{aligned} \tag{166}$$

Now (166) holds for all $\Lambda < \infty$. Thus we need only choose Λ large enough so that

$$\frac{\delta}{A}\,e^{\Lambda\beta/2} > 1$$

to deduce a contradiction. Thus (c) follows.

APPENDIX B

Proof That η is Finite

Define the function

$$g(u_1, u_2) = \frac{r(u_1 \dot{+} u_2)}{r(u_1) + r(u_2)}, \tag{167}$$

where $-A \leqq u_1, u_2 \leqq +A$ and $(u_1, u_2) \neq (0,0)$, and the function $r(u)$ is given by (27). Note that the addition $u_1 \dot{+} u_2$ is performed modulo $2A$. We must show that $\eta = \sup g(u_1, u_2)$ is finite, or that $g(u_1, u_2)$ is bounded.

By assumption (8d), $r(u)$ is continuous, and by assumptions (8c) and (8d) $r(u) > 0$ when $u \neq 0$. Thus $g(u_1, u_2)$ is continuous over its domain. If g is unbounded, let $(u_1^{(n)}, u_2^{(n)})_{n=1}^{\infty}$ be a sequence such that $g(u_1^{(n)}, u_2^{(n)})_n \underset{n}{\rightarrow} \infty$. Then it is easy to see that $(u_1^{(n)}, u_2^{(n)}) \rightarrow (0,0)$. Thus to show that η is finite we need only show that g is bounded in the neighborhood of the origin.

Now let $R_1 = \{(u_1, u_2): u_1, u_2 \geqq 0\}$. We shall show that

$$\eta = \sup_{-A \leqq u_1, u_2 \leqq +A} g(u_1, u_2) = \sup_{(u_1, u_2) \in R_1} g(u_1, u_2). \tag{168}$$

If $(u_1, u_2) \notin R_1$, then either u_1 and u_2 are both negative or u_1 and u_2 have opposite signs. In the first case $g(u_1, u_2) = g(-u_1, -u_2)$, where $(-u_1, -u_2) \in R_1$. In the second case say $|u_1| \geqq |u_2|$, then by assumption (8d) and (8c) $r(u_1 \dot{+} u_2) \leqq r(u_1)$. Thus $g(u_1, u_2) \leqq r(u_1)/[r(u_1) + r(u_2)] \leqq 1 = g(A,0)$ where $(A,0) \in R_1$. Thus we need show only that g is bounded in the neighborhood of the origin where $u_1, u_2 \geqq 0$.

With u_1 and u_2 sufficiently small, the addition $u_1 \dot{+} u_2 = u_1 + u_2$. Also by assumption (8e), we may write

$$r(u) = au^{\alpha}(1 + \epsilon(u)), \tag{169}$$

where $a > 0$, $\alpha > 0$, and $\epsilon(u) \rightarrow 0$ as $u \rightarrow 0$. Thus

$$\begin{aligned} &g(u_1, u_2) \\ &= \frac{a(u_1 + u_2)^{\alpha}(1 + \epsilon(u_1 + u_2))}{a(u_1)^{\alpha}(1 + \epsilon(u_1)) + au_2^{\alpha}(1 + \epsilon(u_2))} \qquad (170) \\ &= \frac{(u_1 + u_2)^{\alpha}}{u_1^{\alpha} + u_2^{\alpha}} \left[\frac{1 + \epsilon(u_1 + u_2)}{1 + \dfrac{u_1^{\alpha}}{u_1^{\alpha} + u_2^{\alpha}} \epsilon(u_1) + \dfrac{u_2^{\alpha}}{u_1^{\alpha} + u_2^{\alpha}} \epsilon(u_2)} \right]. \end{aligned}$$

Now,

$$0 \leqq \frac{u_1^{\alpha}}{u_1^{\alpha} + u_2^{\alpha}}, \qquad \frac{u_2^{\alpha}}{u_1^{\alpha} + u_2^{\alpha}} \leqq 1, \tag{171}$$

so that

$$g(u_1, u_2) = \frac{(u_1 + u_2)^{\alpha}}{u_1^{\alpha} + u_2^{\alpha}} [1 + \epsilon_1(u_1, u_2)], \tag{172}$$

where $\epsilon_1(u_1, u_2) \rightarrow 0$ as $u_1, u_2 \rightarrow 0$. Thus, since

$$0 \leqq \frac{(u_1 + u_2)^\alpha}{u_1{}^\alpha + u_2{}^\alpha} = \frac{\left(1 + \frac{u_2}{u_1}\right)^\alpha}{1 + (u_2/u_1)^\alpha} \leqq 2^{\alpha-1}, \tag{173}$$

we conclude that g is bounded in the neighborhood of the origin, and therefore that η is finite.

Let us remark at this point that discrepancies $r(u)$ do exist for which $\eta = \infty$. For example, $r(u) = \exp(-1/u^2)$. If we set $u_1 = u_2$ and let $u_1 \to 0$ we obtain

$$g(u_1, u_2) = \frac{e^{-1/(2u_1)^2}}{2e^{-1/u_1{}^2}} \to \infty. \tag{174}$$

In this case, of course, $r(u)$ does not satisfy (169) so that $p(u)$ does not satisfy (8e).

APPENDIX C

For channel B, let $V_n(\rho)$ be the volume of the intersection of a sphere in Euclidean n-space of radius ρ and center at the origin with the cube $[-A,A]^n$. For channel D, $V_n(\rho)$ is the volume of $S_n(\mathbf{x},\rho)$ = volume of $S_n(\mathbf{0},\rho)$, where

$$S_n(\mathbf{0},\rho) = \left\{\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n) \in \mathcal{C}_n : d_o(\mathbf{0},\boldsymbol{\alpha}) = \sum_{k=1}^{n} r(\alpha_k) < \rho\right\}.$$

In this appendix we evaluate

$$\lim_{n\to\infty} \frac{1}{n} \ln \frac{(2A)^n}{V_n(an)} = E_a. \tag{175}$$

We shall find E_a by solving an equivalent probability problem: Let $X_1, X_2, \cdots$ be a sequence of random variables uniformly distributed on the interval $[-A,+A]$. Let $Y_n = \sum_{k=1}^{n} r(X_k)$. For channel B, $r(u) = u^2$. It is clear that

$$\Pr[Y_n < \rho] = \frac{V_n(\rho)}{(2A)^n}, \tag{176}$$

hence

$$-\lim_{n\to\infty} (1/n) \ln \Pr[Y_n < an] = E_a. \tag{177}$$

We now make use of

Chernoff's Theorem[15]: Let Z_1, Z_2, $\cdots$ be a sequence of independent identically distributed random variables with moment generating function $E(\exp(Z_i t)) = M(t)$. Let $P_n = \Pr\left[\sum_{i=1}^{n} Z_i \leqq an\right]$, where $a \leqq E(Z_i)$. Then

$$\frac{1}{n} \ln P_n \xrightarrow{n} \ln m,$$

where $m = \min_{t \leqq 0} e^{-at} M(t)$.

If we let $Z_i = r(X_i)$ where X_i is the above random variable, then $Y_n = \sum_{i=1} Z_i$. Thus from (177) $E_a = -\ln m$.

The moment generating function of Z_i is

$$M(t) = E[e^{Z_i t}] = \frac{1}{2A} \int_{-A}^{+A} e^{r(x)t} dx,$$

so that

$$f(t) \triangleq e^{-at} M(t) = \frac{1}{2A} e^{-at} \int_{-A}^{+A} e^{r(x)t} dx, \tag{178}$$

and

$$m = \min_{t \leqq 0} f(t).$$

To minimize $f(t)$, let us differentiate (178) with respect to t:

$$\frac{df(t)}{dt} = 0 = \frac{1}{2A} e^{-at} \left[\int_{-A}^{+A} r(x) e^{r(x)t} dx - a \int_{-A}^{+A} e^{r(x)t} dx\right],$$

so that

$$\int_{-A}^{+A} r(x) e^{r(x)t} dx = a \int_{-A}^{+A} e^{r(x)t} dx. \tag{179}$$

The solution of (179) for t is $t = -\lambda(a)$ where $\lambda(\xi)$ is defined by (19a). With t so chosen

$$m = f(t) = \frac{1}{2A} e^{+a\lambda(a)} \int_{-A}^{+A} e^{-r(x)\lambda(a)} dx,$$

so that

$$\ln m = -\ln 2AK_a(a) + a\lambda(a) \tag{180}$$

where $K_o(a)$ is defined by (19b). Thus

$$E_a = -\ln m = \ln 2AK(a) - a\lambda(a) = C_o(a), \tag{181}$$

where $C_0(a)$ is defined by (19).

If we apply this result to (73) (channel B) with $a = 4\beta$, we obtain $R_{L_2}(\beta) = C_o(4\beta)$. If we apply this result to (113) and (120) (channel D) with $a = \beta$ and $2\eta\beta$ respectively, we obtain $R_U(\beta) = C_o(\beta)$ and $R_L(\beta) = C_o(2\eta\beta)$ respectively. Finally, applying this result to (136) (channel D with quadratic discrepancy) with $a = 2\beta$ yields $R(\beta) \leqq C_o(2\beta)$.

APPENDIX D

Estimate of $C_o(\xi)$ for Small ξ with $r(u) = u^2$

We first obtain an estimate of $\lambda(\xi)$ for small ξ and then show how this estimate can be used to estimate $C(\xi)$.

The quantity $\lambda(\xi)$ is defined by (19a):

$$\int_0^A u^2 e^{-u^2\lambda(\xi)} du = \xi \int_0^A e^{-u^2\lambda(\xi)} du. \tag{182}$$

Observe that $\lambda(\xi)$ monotonically approaches infinity as $\xi \to 0$. Changing the variable of integration in (182) we obtain

$$\int_0^{\sqrt{2\lambda}A} x^2 e^{-x^2/2} dx = 2\lambda\xi \int_0^{\sqrt{2\lambda}A} e^{-x^2/2} dx. \tag{183}$$

Integrating the left integral by parts yields:

$$-xe^{-x^2/2}\Big|_0^{\sqrt{2\lambda}A} + \int_0^{\sqrt{2\lambda}A} e^{-x^2/2} dx = 2\lambda\xi \int_0^{\sqrt{2\lambda}A} e^{-x^2/2} dx. \tag{184}$$

Rearranging terms we obtain

$$\lambda = \frac{1}{2\xi}(1 - \mu(\lambda)) \tag{185}$$

where

$$\mu(\lambda) = \frac{\sqrt{2\lambda}Ae^{-\lambda A^2}}{\int_0^{\sqrt{2\lambda}A} e^{-x^2/2} dx}. \tag{186}$$

Since $\mu(\lambda) \geqq 0$ we have an upper bound on λ:

$$\lambda \leqq 1/2\xi. \tag{187}$$

To obtain a lower bound on λ set

$$\Delta = (1/2\xi) - \lambda. \tag{188}$$

From (185)

$$\Delta = \frac{\mu(\lambda)}{2\xi} = \frac{\lambda\mu(\lambda)}{1 - \mu(\lambda)} = \frac{A\sqrt{2}\lambda^{\frac{1}{2}}e^{-\lambda A^2}}{\int_0^{\sqrt{2\lambda}A} e^{-x^2/2}dx - A\sqrt{2\lambda}e^{-\lambda A^2}} = \frac{N(\lambda)}{D(\lambda)}. \tag{189}$$

It may be verified by differentiation that for $\lambda \geqq 3/(2A^2)$ the numerator $N(\lambda)$ is monotonically decreasing and the denomination $D(\lambda)$ is monotonically increasing so that Δ is monotonically decreasing. With $\lambda = 3/(2A^2)$ we obtain by substitution into (189) $\Delta = 0.76/A^2$ and by substitution into (185), $\xi = 0.22A^2$. Thus for $\xi \leqq 0.22A^2$

$$\lambda = \frac{1}{2\xi} - \Delta \geqq \frac{1}{2\xi} - \frac{0.76}{A^2}. \tag{190}$$

Returning to (189), we may write

$$\begin{aligned} \Delta &\leqq \frac{N\left(\frac{1}{2\xi} - \frac{0.76}{A^2}\right)}{D(3/2)} \\ &\leqq \frac{A(1.12)e^{-A^2/2\xi}\xi^{-\frac{1}{2}}}{0.76} \\ &= 1.35A\frac{e^{-A^2/2\xi}}{\xi^{\frac{1}{2}}}. \end{aligned} \tag{191}$$

Thus we have for $\xi \leqq 0.22A^2$:

$$\lambda = \frac{1}{2\xi} - \Delta \geqq \frac{1}{2\xi}\left[1 - \frac{2.70Ae^{-A^2/2\xi}}{\xi^{\frac{1}{2}}}\right]. \tag{192}$$

Since the quantity $C_o(\xi)$ is defined by

$$C_o(\xi) = \ln 2AK_o(\xi) - \xi\lambda(\xi), \tag{193}$$

where

$$K_o(\xi) = \left[\int_{-A}^{A} e^{-u^2\lambda(\xi)}du\right]^{-1}, \tag{194}$$

we could then use the upper and lower bounds on $\lambda(\xi)$ of (187) and

(192) to obtain an estimate of $C_o(\xi)$. However, this turns out to be a very cumbersome proeedure and we shall side-step this chore. Suffice to observe that $\lambda(\xi)$ approaches $1/(2\xi)$ very rapidly as ξ approaches zero so that for small ξ we could take λ to be $1/(2\xi)$ and obtain

$$C_o(\xi) = \tfrac{1}{2} \ln \frac{2A^2}{\pi e \xi} + \epsilon(\xi), \tag{195}$$

where $\epsilon(\xi) \to 0$ as $\xi \to 0$.

APPENDIX E

Completion of Derivation of Upper Bound on $R(\beta)$ for Channel B

Inequality (86) expresses the fact that

$$R(\beta) \leqq f(\alpha)(1 - 2\hat{\beta}) \tag{196}$$

where

$$f(\alpha) = \frac{\alpha^2}{\alpha^2 - 2} \ln \alpha \tag{197}$$

and α is any integer satisfying $\alpha \geqq 2$, $\alpha^2 > 1/\hat{\beta}$ $(0 \leqq \hat{\beta} < \tfrac{1}{2})$. To obtain the tightest bound we seek to minimize $f(\alpha)$ subjeet to these eonstraints. It may be verified by differentiation that $f(\alpha)$ is a monotone increasing function for integer values of α for $\alpha \geqq 2$. Thus to minimize $f(\alpha)$ we choose α as the smallest integer satisfying $\alpha \geqq 2$, $\alpha^2 > 1/\hat{\beta}$. Thus we ehoose

$$\alpha = 2 \quad \text{when} \quad \tfrac{1}{2} \geqq \hat{\beta} \geqq \tfrac{1}{4},$$

and

$$\alpha = k \quad \text{when} \quad \frac{1}{(k-1)^2} > \hat{\beta} \geqq \frac{1}{k^2}, \qquad (k = 3, 4, 5, \cdots).$$

APPENDIX F

Estimate of $E_B(R)$ for Channel B

Equation (96) expresses the fact that

$$P_{eB}{}^* = \Pr\left[\sum_{i=1}^{n} z_i^2 > \alpha n\right], \tag{198}$$

where the z_i are independent normally distributed random variables

with mean zero and variance N, and $\alpha = \beta(R) = A^2\hat{\beta}(R)$. We seek an expression for $E_B(R) = \lim_{n\to\infty} -(1/n) \ln P_{eB}^*$. We again make use of a form of:

Chernoff's Theorem[15]: Let $Y_1, Y_2, \cdots, Y_n$ be independent and identically distributed random variables with moment generating function $E[\exp(Y_i t)] = M(t)$. Let $P_n = \Pr\left[\sum_{i=1}^{n} Y_i \geqq \alpha n\right]$, where $\alpha \geqq E(Y_i)$. Then

$$\lim_{n\to\infty} (1/n) P_n = \ln m,$$

where

$$m = \min_{t\geqq 0} e^{-\alpha t} M(t).$$

If we set $Y_i = z_i^2$ then $E_B = \lim_{n\to\infty} -(1/n) \ln P_n = -\ln m$. The moment generating function is

$$M(t) = \frac{1}{\sqrt{2\pi N}} \int_{-\infty}^{+\infty} e^{x^2 t} e^{-x^2/2N} dx = \frac{1}{(1-2Nt)^{\frac{1}{2}}} \left(t \leqq \frac{1}{2N}\right).$$

It may be verified by differentiation that the quantity $e^{-\alpha t} M(t)$ is minimized at $t = (1/2N) - (1/2\alpha)$ (which is positive if $\alpha > N$). Thus

$$m = \exp\left[-\alpha\left(\frac{1}{2N} - \frac{1}{2\alpha}\right)\right] M\left(\frac{1}{2N} - \frac{1}{2\alpha}\right).$$

Setting $\alpha = A^2\hat{\beta}(R)$ and taking logarithms we obtain

$$\begin{aligned} E_B(R) = -\frac{1}{n} \ln m &= \frac{\hat{\beta}(R)}{2N} \frac{A^2}{N} - \frac{1}{2} \ln \frac{A^2}{N} e\hat{\beta}(R) \\ &= \frac{\beta(R)}{2N} - \frac{1}{2} \ln \frac{e\beta(R)}{N}. \end{aligned} \tag{199}$$

APPENDIX G

Completion of Asymptotic Estimates for Channel C

1. Let $I_n = \int_0^\theta \sin^{n-2} \varphi \, d\varphi$. We must show that

$E = \lim_{n\to\infty} \frac{1}{n} \ln I_n = \ln \sin \theta$. This is (101a).

(a) $I_n \leqq \int_0^\theta \sin^{n-2}\theta\, d\varphi = (\theta)\sin^{n-2}\theta$, so that

$$\frac{1}{n}\ln I_n \leqq \frac{1}{n}\ln\theta + \frac{n-2}{n}\ln\sin\theta \xrightarrow{n} \ln\sin\theta.$$

(b) $I_n \geqq \int_{\theta-\frac{\theta}{n}}^{\theta} \sin^{n-2}\varphi\, d\varphi \geqq \sin^{n-2}\left(\theta - \frac{\theta}{n}\right)\left[\frac{\theta}{n}\right]$, so that

$\frac{1}{n}\ln I_n \geqq \frac{n-2}{n}\ln\sin\left(\theta - \frac{\theta}{n}\right) + \frac{1}{n}\ln\frac{\theta}{n} \to \ln\sin\theta$. This completes the proof.

2. Let $I_n = \int_0^\psi \sin^{n-2}\varphi\ (\cos\varphi - \cos\psi)d\varphi$. We must show that

$E = \lim_{n\to\infty}\frac{1}{n} I_n = \ln\sin\psi$. This is (101b).

(a) $I_n \leqq \int_0^\psi \sin^{n-2}\psi(\cos\varphi - \cos\psi)d\varphi = \sin^{n-2}\psi[\sin\psi - \psi\cos\psi]$,

so that $\frac{1}{n}\ln I_n \leqq \frac{n-2}{n}\ln\sin\psi + \frac{1}{n}\ln[\sin\psi - \psi\cos\psi] \xrightarrow{n} \ln\sin\psi$

(b) $I_n \geqq \int_{\psi-\frac{\psi}{n}}^{\psi} \sin^{n-2}\varphi(\cos\varphi - \cos\psi)d\varphi$

$$\geqq \sin^{n-2}\left(\psi - \frac{\psi}{n}\right)\int_{\psi-\frac{\psi}{n}}^{\psi}(\cos\varphi - \cos\psi)d\varphi \tag{200}$$

Now $I \triangleq \int_{\psi-\frac{\psi}{n}}^{\psi}(\cos\varphi - \cos\psi)d\varphi$

$$= \sin\psi - \sin\left(\psi - \frac{\psi}{n}\right) - \frac{\psi}{n}\cos\psi$$

$$= \sin\psi - \sin\psi\cos\frac{\psi}{n} + \cos\psi\sin\frac{\psi}{n} - \frac{\psi}{n}\cos\psi.$$

Expanding $\sin(\psi/n)$ and $\cos(\psi/n)$ into power series in (ψ/n) we obtain

$$I = \sin\psi\left[\frac{\psi^2}{2n^2} + o\left(\frac{1}{n^2}\right)\right] = \frac{\psi^2}{2n^2}\sin\psi(1 + o(1)).$$

Thus

$$\frac{1}{n} \ln I = \frac{1}{n} \ln \frac{\psi^2}{2n^2} \sin \psi + \frac{1}{n} \ln (1 + o(1)) \xrightarrow{n} 0.$$

Thus from (200) we have

$$\frac{1}{n} \ln I_n \geqq \frac{n-2}{n} \ln \sin \left(\psi - \frac{\psi}{n} \right) + \frac{1}{n} \ln I \xrightarrow{n} \ln \sin \psi.$$

Thus $E = \ln \sin \psi$ which completes the proof.

APPENDIX H

The Capacity of Channel D

The channel capacity is defined[1] by

$$C = \max_{\hat{p}(x)} [H(y) - H(y \mid x)], \tag{201}$$

where x is the input digit, y the output digit and $H(y \mid x)$ the conditional uncertainty of y given x. The maximization is performed over the input distribution $\hat{p}(x)$. Since $y = x \dotplus z$, $H(y \mid x) = H(z)$ so that

$$H(y \mid x) = H(z) = - \int_{-A}^{+A} p(u) \ln p(u) du,$$

independent of $\hat{p}(x)$. Now $H(y)$ is maximized when the random variable y is uniformly distributed on $[-A, +A]$. Due to the symmetry of the channel, this occurs when $\hat{p}(x) = 1/(2A)$, $-A \leqq x \leqq +A$. In this case

$$H(y) = - \int_{-A}^{+A} \frac{1}{2A} \ln \frac{1}{2A} dy = \ln 2A.$$

Thus the channel capacity is

$$C = \ln 2A + \int_{-A}^{+A} p(u) \ln p(u) du. \tag{202}$$

Writing $p(u) = K_o \exp [-\lambda r(u)]$ we obtain

$$\begin{aligned} C &= \ln 2A + \ln K_o \int_{-A}^{+A} p(u) du - \lambda \int_{-A}^{+A} r(u) p(u) du \\ &= \ln 2AK_o - \lambda N, \end{aligned} \tag{203}$$

where N is defined by (32) or

$$N = \int_{-A}^{+A} r(u) K_o e^{-\lambda r(u)} du. \tag{204}$$

Also, since $p(u)$ integrates to unity,

$$1 = \int_{-A}^{+A} K_o e^{-\lambda r(u)} du, \tag{205}$$

we have

$$\int_{-A}^{+A} r(u) e^{-\lambda r(u)} du = N \int_{-A}^{+A} e^{-\lambda r(u)} du, \tag{206}$$

with N and $r(u)$ specified, λ may be found as the solution to (206). With λ so specified we may find K_o from (205), thus

$$C = \ln 2A K_o(N) - N\lambda(N),$$

where $\lambda(N)$ is the solution of (206) and $K_o(N)$ is the solution to (205). This is the same as $C = C_o(N)$ where $C(\xi)$ is defined by (19).

GLOSSARY OF SYMBOLS

The following symbols are used throughout the paper:

n = dimension of input, output and noise vectors.
$\mathbf{x} = (x_1, x_2, \cdots, x_n)$ = input vector or code word.
$\mathbf{y} = (y_1, y_2, \cdots, y_n)$ = output vector or received vector.
$\mathbf{z} = (z_1, z_2, \cdots, z_n)$ = noise vector.
M = number of words in a code.
$R = (1/n) \ln M$ = transmission rate.
P_{ei} = probability that the receiver makes an incorrect decoding decision when code word i is transmitted ($i = 1, 2, \cdots, M$).
$P_e = (1/M) \sum_{i=1}^{M} P_{ei}$ = over-all error probability.
MDD = minimum discrepancy decoding (always optimum for the channels considered in this paper).
BDD = bounded discrepancy decoding.
P_{eM} = error probability (P_e) using MDD.
P_{eB} = error probability using BDD.
C = channel capacity = "maximum error free rate" using MDD.
$E(R)$ = the best attainable error exponent using MDD, (at rate R).
C_B = bounded distance decoding channel capacity, or "maximum error free rate" using BDD.
$E_B(R)$ = the best attainable error exponent using BDD (at rate R).

The following symbols are used in connection with specific channels:

Channel A

q = the number of symbols in the input, output and noise alphabets.

p_o = the probability that the channel transmits a given symbol correctly.

$d_H(\mathbf{u},\mathbf{v})$ = the Hamming distance between two n-vectors $\mathbf{u}$ and $\mathbf{v}$ = the number of positions in wbich $\mathbf{u}$ and $\mathbf{v}$ differ.

$C(p_o) = \ln q - H(p_o) - p_o \ln (q-1)$ = channel capacity of channel A with symbol error probability p_o.

$H(\rho) = -\rho \ln \rho - (1-\rho) \ln (1-\rho)$ = the entropy function.

d = the minimum distance between code words.

$e = (d-1)/2$ = number of correctable errors in a code with minimum Hamming distance d.

$M(n,d)$ = maximum number of code words in an n-dimensional code with minimum Hamming distance d.

$R(n,d) = (1/n)M(n,d)$ = rate corresponding to $M(n,d)$.

$\beta = d/2n$, a ratio appearing in our bounds.

$t = [(q-1)/q\beta]\,[1 - \sqrt{1 - [2q/(q-1)]\beta}]$, another quantity appearing in our bounds.

$[x]$ = largest integer not exceeding x.

$R(\beta) = \lim_{n\to\infty} R(n,2\beta n)$, asymptotic form of $R(n,d)$.

$\alpha(\rho,p_o) = \rho \ln (\rho/p_o) + (1-\rho) \ln [(1-\rho)/(1-p_o)]$, a quantity appearing in our error bounds.

s = parameter defined by $R = \ln q - H(s) - s \ln (q-1) = C(s)$

Channel B

A = maximum amplitude of input coordinates.

N = variance of normally distributed noise coordinates.

$d_E(\mathbf{u},\mathbf{v}) = \sum_{i=1}^{n} (u_i - v_i)^2$ = Euclidean distance between the n-vectors $\mathbf{u}$ and $\mathbf{v}$.

d = the minimum distance between code words.

$M(n,d^2)$ = maximum number of code words in an n-dimensional code with minimum Euclidean distance d.

$R(n,d^2) = (1/n) \ln M(n,d^2)$ = rate corresponding to $M(n,d)$.

$\beta = d^2/4n, \hat{\beta} = \beta/A^2$, ratios appearing in our bounds.

$R(\beta) = \lim_{n\to\infty} R(n,4\beta n)$, asymptotic form of $R(n,d^2)$.

$R_L(\beta)$ and $R_U(\beta)$ = lower and upper bounds on $R(\beta)$ given by (18) and (19) respectively.

The function $C_o(\xi)$, $0 < \xi < A^2/3$, is defined as follows: $\lambda(\xi)$ is the quantity defined by

$$\int_0^A r(u)\, e^{-\lambda(\xi) r(u)} du = \xi \int_0^A e^{-\lambda(\xi) r(u)} du$$

where $r(u) = u^2$, and

$$K(\xi) = \left[\int_{-A}^{A} e^{-\lambda(\xi) r(u)} du \right]^{-1}.$$

Then

$$C_o(\xi) = \ln 2AK_o(\xi) - \xi\lambda(\xi).$$

Channel C

P = $(1/n) \times$ the energy of a code word.
N = variance of the normally distributed noise coordinates.
$d_E(\mathbf{u},\mathbf{v})$ = the Euclidean distance between $\mathbf{u}$ and $\mathbf{v}$.
$a(\mathbf{u},\mathbf{v})$ = the angle between n-vectors $\mathbf{u}$ and $\mathbf{v}$.
θ = the minimum angle between code words.
$M(n,\theta)$ = maximum number of code words in an n-dimensional code with minimum angle θ.
$R(n,\theta)$ = $(1/n) \ln M(n,\theta)$ = rate corresponding to $M(n,\theta)$.
ψ = $\sin^{-1} \sqrt{2} \sin (\theta/2)$, a quantity appearing in our bounds.

Channel D

$\mathcal{C}_n$ = set of real n-vectors $\mathbf{u} = (u_1, u_2, \cdots, u_n)$ satisfying $|u_k| \leqq A$.
$\dot{+}, \dot{-}$ = addition and subtraction modulo $2A$ (with result reduced into the interval $[-A,+A]$).
$p(u)$ = noise probability density function.
$r(u)$ = $(1/\lambda) \ln [p(0)/p(u)]$ $(-A \leqq u \leqq +A)$, quantity related to the discrepancy.
$d_o(\mathbf{u},\mathbf{v}) = \sum_{k=1}^{n} r(u_k \dot{-} v_k)$ = discrepancy between n-vectors $\mathbf{u}$ and $\mathbf{v}$ belonging to $\mathcal{C}_n$.
N = $E(r(z))$, a parameter associated with the noise density $p(u)$.

$C_o(\xi)$, defined exactly as for channel B but with the appropriate $r(u)$ used instead of u^2.

$\eta = \sup_{-A \leqq u_1, u_2 \leqq A} \dfrac{r(u_1 + u_2)}{r(u_1) + r(u_2)}$, a quantity appearing in our bounds.

ACKNOWLEDGMENT

The author wishes to thank L. A. Shepp, E. N. Gilbert, and especially D. Slepian for many stimulating discussions and helpful suggestions.

REFERENCES

1. Shannon, C. E., A Mathematical Theory of Communication, B.S.T.J., *27*, July and October, 1948, pp. 379–423, 623–656.
2. Elias, P., Coding for Two Noisy Channels, in *Information Theory*, Colin Cherry (ed.), Academic Press, New York, 1956, pp. 61–74.
3. Gallager, R. G., *Low Density Parity Check Codes*, MIT Press, Cambridge, 1963.
4. Gramenapoulos, N., An Upper Bound for Error-Correcting Codes, M.S. Thesis, Department of Electrical Engineering, MIT, 1963.
5. Bose, R. C., and Ray-Chaudhuri, D. K., On a Class of Error Correcting Binary Group Codes, Information and Control, *3*, 1960, pp. 68–79.
6. Hamming, R. W., Error Detecting and Error Correcting Codes, B.S.T.J., *29*, April, 1950, pp. 147–160.
7. Shannon, C. E., Certain Results in Coding Theory for Noisy Channels, Information and Control, *1*, 1957, pp. 6–25.
8. Peterson, W. W., *Error Correcting Codes*, MIT Press and John Wiley & Sons, New York, 1961.
9. Plotkin, M., Binary Codes with Specified Minimum Distance, IRE Transactions on Information Theory, *IT-6*, 1960, pp. 445-450.
10. Wolfowitz, J., *Coding Theorems of Information Theory*, Prentice-Hall, Inc., Englewood Cliffs, 1961.
11. Shannon, C. E., Probability of Error for Optimal Codes in a Gaussian Channel, B.S.T.J., *38*, May, 1959, pp. 611–656.
12. Wyner, A. D., An Improved Error Bound for Gaussian Channels, B.S.T.J., *43*, November, 1964, pp. 3070–3075.
13. Rankin, R. A., The Closest Packing of Spherical Caps in n-dimensions, Proceedings of the Glasgow Mathematical Association, *2*, 1955, pp. 139–144.
14. Blachman, N. M., On the Capacity of a Band-Limited Channel Perturbed by Statistically Dependent Interference, IRE Transactions on Information Theory, *IT-8*, 1962, pp. 48–55.
15. Chernoff, H., A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the Sum of Observations, Annals of Math. Stat., *23*, 1952, pp. 493–507.